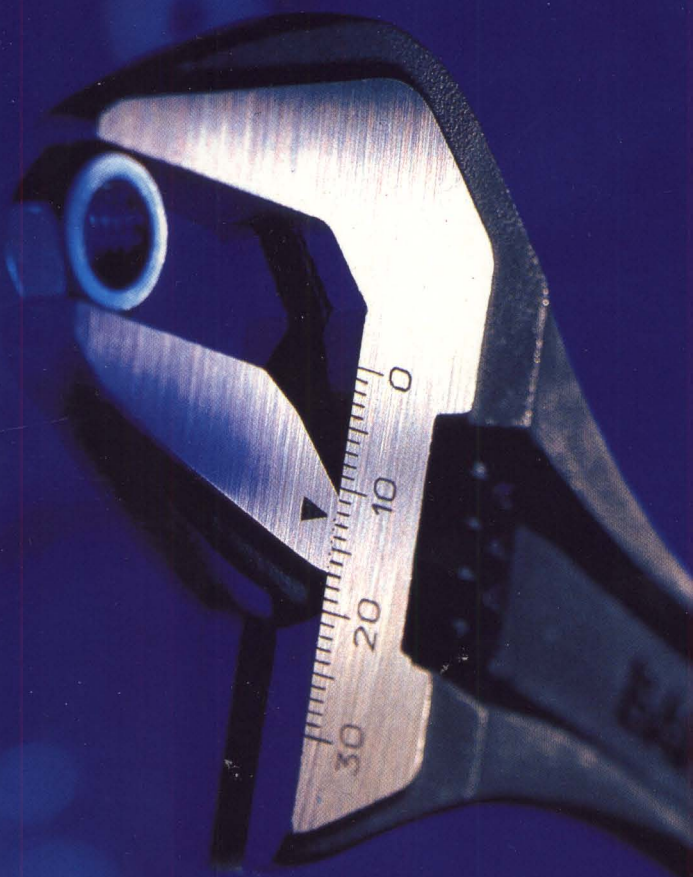
DR SOLOMON'S

Virus Encyclopaedia



Dr Solomon's Virus Encyclopædia

Dr. Alan Solomon & Dmitry O. Gryaznov

D' SOLOMON'S

S&S International PLC
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK.
Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777 BBS: +44 (0)1296 318810

COPYRIGHT

Dr. Solomon's Anti-Virus Toolkit is copyright © 1995 S&S International PLC. All rights reserved. Dr. Solomon's Anti-Virus Toolkit is protected by the copyright laws which pertain to computer software. It is illegal to make copies of the program other than for your own use without written permission from S&S International PLC. No part of the manual or other documentation accompanying Dr. Solomon's Anti-Virus Toolkit may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form or by any means, without the prior written permission of S&S International PLC.

© 1995 S&S International PLC

ISBN 1 897661 00 2 Dr. Solomon's Virus Encyclopaedia

DISCLAIMER

Neither S&S International PLC nor anyone else who has been involved in the creation, production or delivery of Dr. Solomon's Anti-Virus Toolkit or this manual makes any warranties with respect to the contents of the software or this manual and each specifically disclaims any implied warranties of merchantability or fitness for any purpose. S&S International PLC reserves the right to revise the software and the manual and to make changes from time to time in the contents without obligation to notify any person.

TRADEMARKS

Dr. Solomon's Anti-Virus Toolkit and VirusGuard are registered trademarks of S&S International PLC. All other product names mentioned are acknowledged to be the marks of their producing companies.

SUPPORT

Support for this program is freely available from S&S International PLC in the following ways:

By mail: S&S International PLC, Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK

By telephone: +44 (0)1296 318733

By fax: +44 (0)1296 318734

By BBS: +44 (0)1296 318810

E:mail: support@sands.co.uk

Contents

1	About viruses	1
2	Virus prevention	13
3	Networks and viruses	16
4	A brief history of viruses	18
5	Mechanisms of stealth	34
6	Polymorphic viruses	39
7	PC Viruses	44
	The virus naming problem	44
	Removal methods	46
	The viruses	47
Index		269

"To see a World in a Grain of Sand
And a Heaven in a Wild Flower
Hold Infinity in the palm of your hand
And Eternity in an Hour."

William Blake – *Auguries of Innonence*

Also to be found in the Maltese Amoeba virus

1 About viruses

What is the first thing to do?

Don't panic. Indeed, don't do anything. Have a cup of tea or coffee – don't start bashing away at the keyboard before you've determined what you ought to do. In my experience, a lot of the 'damage done by viruses' is actually damage done by people doing things before they've made sure of what they ought to do, which is another way of saying panic. So, don't panic.

What is a virus?

A virus is a program that copies itself.

That's the definition of a virus. In retrospect, it's unfortunate that the word 'virus' was used – it makes the problem sound a lot worse than it is, and people get the plural wrong (the plural is not 'viri' or even 'virii', it's 'viruses'). It might have been better to use the word 'weed'. But we're stuck with 'virus'.

A virus need do no more than replicate in order to be a virus – indeed, 95% of viruses do no more than that, plus some trivial extra like beeping the keyboard, or displaying a message. And conversely, if a program does something nasty that you weren't expecting, that doesn't make it a virus, unless it replicates. Such a program is called a 'trojan', after the famous horse of Troy.

Why are viruses bad news?

If a virus does nothing but copy itself, why do people get so worked up when they have one? For example, ***Form*** virus beeps every time you hit a key on your keyboard on the 18th of each month, so why does everyone who gets infected want to get rid of it? There are a few reasons for this. If you don't get rid of the virus, there is a strong likelihood that eventually you'll pass it on to a supplier or customer, who will be upset. Over 99% of viruses that actually spread in the wild are memory resident, so there is the possibility of incompatibilities between the virus and some other program you are running (for example, ***Jerusalem*** tries to use one of the resources that Novell uses, so you can't run both Novell and ***Jerusalem*** on the same system). Thirdly, even though we have analysed and documented the virus, the user might remain nervous that the virus does more than has been documented, or that he has a different version of the virus. So in almost every case that we have seen, people want very much to get rid of the virus (apart, sometimes, for keeping one specimen for a 'zoo').

If you do get rid of the virus, this is going to take time, and time is money. Each PC will take at least several minutes, and each floppy disk will take at least several seconds (and there may be a lot of floppy disks). It would be nice if you only had to worry about those computers and floppies that are infected, but of course you don't know which ones these are until you've done the virus-hunt, so you have to check everything.

Things that are not viruses

Bugs

Bugs are not viruses, and viruses are not bugs. I am using a word processor that I know has a serious bug. If you work with a large file for a long time, then eventually something goes wrong inside the program, and it refuses to let you save the file to the disk, so that you lose all the work you've done since the last save. This program comes from a major software house, and they didn't do this on purpose, so it isn't a trojan. The programmers made a mistake. Programmers are human, and humans make mistakes. Programmers, like other humans, have pride, and don't like to admit that they make mistakes, so they call them 'bugs', as if the bug had drifted in through the window and settled on the program. All sufficiently complex programs have bugs.

Anti-virus software does not detect bugs. If it did, it would report bugs in just about everything.

False alarms

False alarms are not viruses. A false alarm is when you think you have a virus, but you are mistaken. Sometimes, people have some hardware or software fault, and after running some diagnostics, eliminate the possibility of hardware or software problems, conclude that it is therefore a virus, and proceed on that assumption. More often, a false alarm is the result of running anti-virus software.

Anti-virus software, in common with other software, is not infallible. The two main mistakes that an anti-virus program can make are to fail to find a virus that is there (I once tested a program that failed to find any boot sector viruses whatsoever, and these account for over two thirds of infections) or to claim that a virus is present when there isn't one, and that is called a false alarm.

When an anti-virus program gives a false alarm, it looks pretty much like the real thing. There are a couple of things that might indicate that the alarm is false, though.

1. Only one file is giving the alarm (or perhaps four files, but they are copies of the same file).
2. Only one product gives the alarm – other products say the system is clean.
3. You get the alarm after running multiple products, but not when cold-booting and running any one product.
4. The virus that is detected is not listed as in the wild (of course, this list changes all the time).

Unfortunately, there's no hard rule that can be applied. You can't say it's a false alarm if one of the four above is true, or if all four of the above are true. The only way to really nail down a false alarm is to send the suspect file to the product vendor giving the alarm, and ask them to verify that it is a virus by analysing it in their virus lab. And this might take some time.

Meanwhile, a false alarm can be as much hassle as a real virus, or even more. If you have a floppy disk that is infected with ***Stoned*** virus, you can simply copy the data off the disk and destroy the infected floppy, or you can get rid of the virus with your anti-virus program, or demand a replacement disk. Whatever, the cost is just a few seconds. But if you get an update of you favourite anti-virus program, and it tells you that you have ***Stoned*** virus on one of the files on your file server, then resolving the situation will take longer. You know and I know that ***Stoned*** cannot infect files. But just maybe someone has written a file virus and someone has decided to call it ***Stoned*** (for example, there are two unrelated viruses, one called ***Parity*** and the other called ***Parity Boot***). So, you send the file to your product vendor for analysis and comment. Meanwhile, to be safe, you remove the file from the server (or possibly the product is barring access to that file). This might mean that some important system won't work any more, as it needed that file. It also means that you have to keep track of the response to the problem, report it up through the usual security breach reporting channel, and so on. You might try deleting the offending file and re-installing the software that is causing the false alarm, but when you've finished doing that you still get the false alarm.

It isn't surprising that some people have changed their anti-virus software after too many false alarms.

Anti-virus software does not detect false alarms – if it did, it wouldn't report the false alarm, would it?

Jokes

A joke is something that is funny. Of course, what one person finds funny is not the same as what another person finds funny – it depends on your sense of humour. A program that pretends to format your hard disk, and then reveals that it hasn't – is that funny? It depends on your sense of humour.

Some people love to play practical jokes, and on certain dates one must apply a little scepticism to alleged virus reports. Some anti-virus software detects jokes, and tells you 'You have a joke called ....'. The reason for this, is that some jokes are fairly widespread, and are known to cause concern, so the anti-virus is trying to calm things down, by saying 'Yes, I know about this, and it's harmless'.

Trojans

A trojan is a program that does something more than the user was expecting, and that extra function is damaging. This leads to a problem in detecting trojans. Suppose I wrote a program that could infallibly detect whether another program formatted the hard disk. Then, can it say that this program is a trojan? Obviously not – if the other program was supposed to format the hard disk (like Format does, for example), then it is not a trojan. But if the user was not expecting the format, then it is a trojan. The problem is to compare what the program does with the user's expectations. You cannot determine the user's expectations for a program.

So, we have to make some judgements. The Aids Information Diskette is generally considered to be a trojan. About 20,000 copies of this were mailed to users in 1989, purporting to be a program that teaches you about Aids. In fact, it was a trojan – after you reboot your computer 90 times, it encrypts and hides all the filenames on your hard disk, and demands that you pay for your licence to use it. Although the documentation that came with it told you that something bad was likely to happen, it is generally considered to be a trojan. Format is not a trojan.

As a rule, you don't see trojans very often – they don't copy themselves, and don't spread in the way that viruses do. Trojans are not a real threat, except in one of the following circumstances:

1. When they are widely disseminated, like the Aids Information Diskette.
2. They are targetted on an organisation, in which case it is an 'inside job', done by an employee.

Some anti-virus products detect a few trojans (such as the Aids one), but most products don't detect trojans at all.

Corrupted programs

Some files are simply corrupted (perhaps by a hardware problem), and hang the computer when run. For some reason, these sometimes end up in virus collections, unless the collection is carefully maintained.

Intended viruses

Some virus authors are less skilful than they would like to be, and write what is clearly intended to be a virus, but for some reason there is such a major bug that the virus does not work at all. They release these, however, in the fond belief that no-one will ever test them (or perhaps they didn't test them themselves). One typical mistake is to get confused about decimal versus hexadecimal, and so their source code presumably says 'int 21' for the DOS function interrupt, but it should have said 'int 21h' (which is 33 in decimal).

Droppers

A dropper is a program that is not a virus, nor is it infected with a virus, but when run it installs a virus into memory, on to the disk, or into a file. Droppers have been written sometimes as a convenient carrier for a virus, and sometimes as an act of sabotage. Some anti-virus programs try to detect droppers.

Germs

A germ is an instance of the virus in generation zero, and in such a form that the infection could not have happened naturally. For example, a virus that only infects files larger than 5Kb, but infecting a tiny 10-byte file. Alternatively, it might be an instance of the virus without any host file – if you remove the virus, you are left with a zero-byte file. This is the original file created by the virus author.

Different kinds of virus

Boot sector viruses

The commonest kinds of virus are boot sector viruses, such as ***Form*** and ***Stoned.*** These infect the boot sectors of floppy disks, and either the MBR (Master Boot Record, or Partition sector) or the DBR (DOS Boot Record, or DOS boot sector) of hard disks. Here's how a BSV spreads.

A floppy diskette has just arrived, with some data on it (some word-processed files and a spreadsheet, perhaps). This is part of a project that you are doing jointly with a colleague. What your colleague doesn't know is that his computer is infected with a BSV, and therefore so is the diskette he sent you. You put the diskette in drive A: and start using these files. So far, the virus hasn't done anything. But when you finish for the day, you switch off the computer and go home. Next day, you come in and switch on. The floppy disk is still in drive A:, so the computer tries to boot up from there. It loads the first sector into memory and executes it (normally, this is a little program written by Microsoft to load DOS), or if it can't find DOS on the diskette, to

tell you so – 'Not a system disk, please press any key to continue'. Everyone has seen this message numerous times, and so you open the drive door and press a key.

But this diskette is infected with ***Stoned***, so what executed was not just the program by Microsoft, but the ***Stoned*** virus, written in 1987 in New Zealand (and so sometimes called the New Zealand virus). The virus installs itself on the hard disk, replacing the MBR, and copying the original MBR to a place a little further down the disk.

When you start up from the hard disk, the MBR runs, but this is ***Stoned*** virus. ***Stoned*** virus goes memory resident, capturing the diskette read/write interrupt 13h, and then it loads the original MBR, and the boot-up process continues as normal. But, since the diskette read/write interrupt is captured, every time any write or read access (you think you're making a read, but the virus decides to write anyway) is made to drive A: the floppy is examined, and if it is not already infected, ***Stoned*** virus is installed on the boot sector. Thus, your computer is now infecting every diskette put in drive A:, and sooner or later one of these will be sent to a colleague, and the cycle continues.

The detail of various BSVs is different, but the principle is the same. They are carried by the boot sectors of infected diskettes, and only in that way (a BSV cannot spread across a network, for example). And the only way to get infected is to try to boot from an infected diskette, even if the boot fails.

BSVs infect PCs. They don't care what operating system is running, or what security software is installed, because at the time the BSV installs itself the operating system or security program is not running yet. However, with some non-DOS operating systems, although the PC is infected the virus cannot copy itself on to subsequent diskettes and cannot spread. It can, however, still do damage, as was discovered by one surprised Unix user when ***Michelangelo*** went off on March 6th.

To most people, the fact that viruses can infect in this way comes as a big surprise, which partly accounts for BSVs being so common.

TSR File viruses

The second commonest kind of virus is the TSR file virus. As the name suggests, these infect files. These are usually COM and EXE, but there are some device driver viruses, some viruses infect overlay files, and executable programs don't always have the extension COM or EXE, although over 99% do.

For a TSR virus to spread, someone has to run an infected program. The virus goes memory resident, and typically looks at each program run thereafter and infects it if it is not already infected. Some viruses are called 'fast infectors', and they infect if you just open the file (for example, a backup might open every file on the drive) – ***Dark Avenger*** was the first fast infector. In the case

of *Green Caterpillar*, the infection trigger is anything that determines what files are present (such as DIR). Other triggers have been used, but the commonest is to infect each program that you are about to run.

Non-TSR file viruses

It is much easier to write a non-TSR virus, and so many of the budding virus authors do so. But it is quite rare for such a virus to be encountered in the wild – less than 1% of reported outbreaks are a non-TSR virus. With such a virus, running an infected program runs the virus, which at that time looks for another file to infect, and infects it. *Vienna* is the commonest non-TSR virus; *Vienna* was the first file virus in the wild, and is still reported occasionally. There are a lot of viruses based on *Vienna*, because a disassembly (which is almost equivalent to source code) was published in a book in 1987.

Companion viruses

If you have a COM file and an EXE file with the same filename and type that name, DOS runs the COM file in preference to the EXE file. Companion viruses use this fact – each EXE file that you have acquires a companion COM file with the same name. Then, when you try to run your EXE program, actually the COM program runs, and that is the virus. When the virus has finished doing what it wants to do (such as creating another companion for another file), it then runs the EXE program, so that everything seems to work normally.

There have been a few successful companion viruses, but not many. The main advantage to the virus author is that because the EXE file does not change, some change-detection software might not realise that a virus is spreading.

Another type of companion is the 'path companion'. This sort of virus puts a program in a directory that is earlier in the DOS PATH than is the victim. When you run a program that is not in your current subdirectory, DOS searches for the program in various subdirectories, as specified by the PATH command in your AUTOEXEC.BAT file. Path companions are harder to write than ordinary companions, so there aren't many of them.

Overwriting viruses

An overwriting virus simply overwrites each file it infects with itself, and the program no longer functions. Because this is so glaringly obvious, overwriting viruses are never successful in spreading.

Multipartite viruses

Some viruses, such as ***Tequila***, infect multiple objects. When you run a ***Tequila***-infected EXE, ***Tequila*** installs itself on the MBR. When you boot up the computer, ***Tequila*** runs from the MBR, and goes memory resident. While ***Tequila*** is memory resident, it infects EXE files.

Other viruses, such as some of the versions of ***Anticad***, infect COM, EXE and MBRs interchangably. Some viruses infect COM, EXE, MBRs and device drivers.

Miscellaneous objects of infection

There is a virus that infects OBJ files. There is a virus (***Starship***) that infects by creating a new DBR, leaving the old one intact, leaving the code on the MBR intact, and changing the pointer in the MBR so that the ***Starship*** DBR is executed before the original DBR. There is another virus (***DIR II***) that infects file systems by changing the FAT and directories so that files on the hard disk are all cross linked to the virus.

There are all sorts of ways of skinning this particular cat.

Virus characteristics

Fast

As explained above, a fast infector spreads rapidly within a computer by infecting everything that is accessed. A fast infector isn't as bad as it sounds – it is just as easy to clean a computer with 1000 infected files as one with 10, provided you have an anti-virus program that does a good cleaning job. However, most anti-virus products check memory for viruses, and the possibility of a fast infector in memory is one of the reasons why. If there is a fast infector in memory, and the product opens all your files, you wind up with every file on the computer infected.

Slow

The opposite of a fast infector is a slow infector. The idea here is that if the virus spreads slowly, you're less likely to notice it and kill it. There are various ways that a slow infector can work, but the classic slow infector works by only infecting those files that you had intended to change anyway. This means that if you are running a change detector as an anti-virus measure, the change detector will trigger each time there is an infection, but since you had intended the file to change anyway, you'll tell it to accept the change.

Starship is another way of doing a slow infector – it only infects files as you copy them from your hard disk. So no file on the hard disk ever changes, and the change detector is happy. But when you copy a file to a floppy, the copy is infected, and when you take this to another computer protected by the change detector, the change detector warns you of the existence of the new file. You will then reassure the change detector that you knew about the new file, and the change detector is happy, and another system is infected.

Stealth

If a virus is memory resident (as are over 99% of viruses in the wild), then it has hooked at least one of the interrupts. If it is a BSV, then it has hooked the disk read/write interrupt 13h. If it is a stealth virus, and any program that tries to read the boot sector, then the virus says 'Aha, someone wants to see the boot sector – I'll just read the original boot sector from where I put it, and present that instead'. So the software sees nothing out of the ordinary. ***Brain,*** vintage 1986, was the first virus that used this trick. File viruses can use a similar trick to disguise their presence, so that any software reading the file only sees the bytes that were there before the virus came along – ***Frodo*** is an example of this. It is much commoner to see stealth in BSVs than in file viruses, as it is much easier for the virus author to implement stealth in a BSV.

Stealth is covered in more detail later on – see 5 Mechanisms of stealth.

Polymorphism

The commonest kind of anti-virus program that people use is the scanner, looking for a repertoire of viruses. So for the virus author this is the kind of product that he would most like to defeat. A polymorphic virus is one where if you take two instances of the virus, there are no bytes in common between them, so you cannot write down a byte-sequence and go looking for that in order to detect the virus. You have to do something a lot more complex and difficult.

Polymorphic viruses are covered in more detail later on – see 6 Polymorphic viruses.

Damage done by viruses

We can categorise the damage done by viruses into six groups, according to the severity of the damage. Some authorities postulate the possibility of a virus that actually does good, but no-one has yet demonstrated such a virus.

We define damage as: the virus does something that you'd rather it hadn't done; and we quantify damage by measuring how long it takes to put things back the way they ought to be.

We don't include consequential damage in this categorisation (damage done by the user in a mistaken attempt to get rid of the virus). It is remarkable how many people will format the hard disk to get rid of ***Stoned,*** for example. All this does is get rid of all your data – the virus is untouched, as it resides in the MBR, which is not touched by Format. Nor can we include damage done by obscure incompatibilities between the virus and the system. For example, if a computer that was originally set up under DOS v2 (but is now running a later DOS) is infected by ***Stoned,*** then a large number of files will be corrupted because the design of the virus had not anticipated this situation.

Trivial damage

This is done by a virus such as ***Form*** (the commonest virus in the world). On the 18th of every month, each key that you hit makes the speaker beep. All you need to do is to get rid of the virus. This will usually take seconds or minutes (per computer).

Minor damage

A good example of minor damage is the way that ***Jerusalem*** virus deletes any program that you try to run after the virus has gone memory resident on Friday the thirteenth. At worst, you will have to reinstall some programs, so the damage is unlikely to be more than 30 minutes per computer.

Moderate damage

If a virus formats the hard disk, scrambles the FAT or overwrites the hard disk, this is moderate damage. The damage is only moderate because you know that it has happened, and you can reinstall DOS and reload yesterday's backup, because you do a backup every day. So, you'll lose on average half a day's work, plus maybe an hour doing the reinstall and restore. The virus most famous for moderate damage is ***Michelangelo.***

Major damage

This is where a virus hits your backups as well as your hard disk. Every 16th time that a ***Dark Avenger***-infected file is run it overwrites a random sector on the hard disk with 'Eddie lives ... somewhere in time'. This might have been going on for several weeks. You discover ***Dark Avenger,*** get rid of the virus, and find 'Eddie lives' at several places in several files. You restore yesterday's backup, and find 'Eddie lives' in those as well. You might have to go back a few weeks before you can find clean data files, and when you've restored a six week old backup, you'll find that you don't actually have any way to redo that work, because you don't have the original documents to work from.

Severe damage

Severe damage is done when a virus makes gradual and progressive changes (so that backups are also corrupted), but the changes are not obvious (there is no 'Eddie lives' to look out for). You wind up simply not knowing whether your data is correct or changed.

Unlimited damage

Some viruses (such as *Cheeba, Vacsina.44.login* and *GP1*) aim to get the system manager password and pass it along to a third party. In the case of *Cheeba,* for example, it creates a new user with maximum privilege, with a fixed user name and password. The damage is then done by the third party person, who can log in to the system and do anything he likes.

How viruses are spread

It seems to be a common belief that viruses are spread by games, by shareware or by BBSes. The truth is more complex. First, remember how the most common sort of virus, boot sector viruses, work – a physical diskette has to be involved, and there doesn't need to be any software on it. You cannot get a BSV by using a BBS.

The most likely routes by which a virus gets into an organisation are engineers and parents.

1. Hardware engineers visit a large number of computers, and like the busy little bee, could pick up some pollen here, and deposit it there. Hardware engineers should have all their software diskettes permanently write protected, but don't. Hardware engineers should frequently check any write enabled diskettes for viruses, but don't. Of course, the majority of hardware engineers are clean and well behaved, but there are a few that need re-education.

2. Parents have children, and if there is a PC at home, and the children are young teens, then they quite possibly swap software at school. The diskettes that they bring home might well be infected, and if the parent is taking diskettes to and from work, he could easily take a virus into work with him.

3. A boot sector virus could arrive on a data diskette from a colleague.

Other ways of getting a virus include:

In shrink-wrapped software – some of the largest companies have accidentally shipped a virus in shrink-wrapped software.

Along with purchased hardware – most hardware comes with diskettes containing utilities or drivers.

Salesmen running demos could unwittingly install the virus they picked up from the last place they ran their demo.

2 Virus prevention

We recommend that everything be virus checked before it is used – this includes floppy disks with data on (remember BSVs) as well as software. This could be done using a scanner such as **FindVirus,** which could be installed on every computer (for convenience, because if it isn't convenient, it won't get done) or it could be installed on designated sheep-dip computers, which is more convenient for the PC Support people to keep up to date, but less convenient for the users. Alternatively, you can make the whole thing as transparent and painless as possible by installing a TSR scanner (such as **VirusGuard**) which means that everything is automatically scanned without the user being aware of it (unless, of course, a virus is found). The TSR scanner is the route that most people choose, together with some dedicated sheep-dip machines.

Rules, procedures, education and tools

Linda had worked in her job for some years. She occasionally took work to do on her home PC, with the knowledge and approval of her supervisor. One day, the PC Support department found a virus on her office PC. Later the same day Linda was fired for bringing a virus on to the premises.

Linda was very upset at what she saw as unfair dismissal and sued the company. She won because the company she worked for had no rules to tell employees what to do (so she hadn't broken any rules). Although they had anti-virus software, there were no procedures for checking incoming disks (so she hadn't failed to carry out company procedures). On investigation, it looked highly likely that the PC Support department had accidentally infected her machine, and only discovered it when they sent diskettes, copied on Linda's machine, to another company, who did check for viruses and found one on those diskettes.

If such procedures had been in place and Linda had ignored them, then the company would have had a good reason for firing her. Of course, with proper rules and procedures, they would probably not have been infected by a virus in the first place.

But you have to acknowledge the fact that people behave the way that they do. If you make your anti-virus procedures onerous and difficult, they'll quite likely be ignored on the grounds that viruses are very rare, and the cost and hassle of the procedures is too great.

A good set of rules might be as follows:

1. Any incoming floppy disk must be virus-checked.

2. If your anti-virus software finds a virus, tell PC Support.

Notice that the rules are very simple – that way, people are more likely to remember and follow them.

The next thing you need is procedures. The procedure tells the users how to obey the rules. The procedure for checking disks should be written down in detail – 'Put the floppy disk in the drive, and type ...'. If you have a sheep-dip computer, put the procedure up on the wall near to it.

Education is also important. You can't just tell grown-ups to do something and expect that they'll obey without question. You have to explain the reason to them. You can do this with talks, or by getting the Virus Video[1] and letting them watch it.

You also have to provide tools – you can't detect a virus with your bare hands.

Anti-virus tools

Scanners

A scanner is a program that knows how to find a particular repertoire of viruses. Scanners are updated, quarterly or monthly. For many users, quarterly upgrades are sufficient, but every now and then, a new virus comes out and spreads very fast (such as ***Tequila***, or ***Smeg***). In that case, you could be unable to detect this in-the-wild virus for several weeks, depending on where you are in the update cycle. So, many people subscribe to monthly upgrades to avoid this situation.

Scanners can be either command line, or TSR. **FindVirus** is a command line scanner, and must be run by the user (this could be done at start-up in the AUTOEXEC.BAT). **VirusGuard** is a TSR scanner, and works continuously. As soon as any diskette is accessed, it is checked for boot sector viruses, and as soon as any file is used, it is checked for file viruses. Because it is a TSR, there is a slight reduction in free memory (about 6Kb) and a slight hesitation each time an executable file is loaded. Also, in common with other TSR scanners, it doesn't have the full facilities of the command line version (to economise on memory consumption), so it cannot do virus repair, and it cannot detect a tiny percentage of viruses (the extremely polymorphic ones).

---

1 Dr. Solomon's Virus Video in either 'The Personal Video' or 'The Corporate Training Pack' by S&S International PLC.

Checksummers

A checksummer is a change detector. Executable files should not change, except for a good reason such as updating of the software. A checksummer aims to detect changes. The advantage of checksummers is that they do not detect a repertoire of viruses, so do not need updating. The downside of checksummers, is that they are more hassle than scanners (files change on your computer more often than you might have thought, for good and valid reasons), and that they do not detect all viruses. For example, checksummers do not detect slow viruses, they do not detect all boot sector viruses (if the hard disk code is left unchanged) and they have problems with stealth viruses. Some people use checksummers, but they are a minority.

Checksummers can be command line (like **ViVerify**), or TSR (like **Certify**). The advantage of a TSR checksummer is that it can prevent any software from being run unless it is known to the checksummer.

3 Networks and viruses

A network is a group of computers connected together to make it easier to share data. This provides interesting opportunities for viruses, and for dealing with viruses.

There is a common perception that once a virus gets on to a network, somehow it flashes round the whole network very quickly. The truth, of course, is more complex. Firstly, BSVs cannot travel across networks – if several machines on a network are infected, that's because the virus spread via floppy disks in the usual way. Here's how a file virus spreads across a network.

1. User 1 gets his computer infected, perhaps by a salesman's demo diskette. The virus goes TSR.
2. User 1 runs other programs on his hard disk. They get infected.
3. User 1 runs some programs on the network. They get infected. A network emulates a DOS device – reading and writing to files on the server is done in exactly the same way as locally. The virus doesn't have to behave any differently to infect files on the server.
4. User 2 logs on to the server, and runs an infected file. The virus is now TSR in user 2's machine.
5. User 2 runs several other programs, on their local hard disk, and on the server. Each file becomes infected.
6. User 3, user 4 and user 5 log on and run infected files.
7. And so on.

Network protection

70% of networks use Novell, so we'll use that as an example, but you can adapt the same principles for other network operating systems.

1. You can make directories read-only. If you make files on the local hard disk read-only, you're wasting your time, because just about every file virus will make them read/write, infect them, and make them read-only again. This is because the user has the privilege to make files read/write on his local hard disk. But on a file server, you don't have to give that privilege to the user, and the virus has the same privilege as the user. Indeed, the virus is the user, and can do no more than the user can – there is no magic about viruses – they are subject to the same constraints as any other programs.

Unfortunately, some packages can't be run from read-only subdirectories, because they want to write to configuration or temporary files in the same directory.

2. You can make programs execute-only. This means that although the directory is read/write, the executables cannot be written to, or even read. They can only be run. Be warned, though, that on Novell this is a one-way street – once you've made a file execute-only, you can't go back. All you can do is delete it, even if you are Supervisor. So, make a copy first. Some programs won't run if they are execute only, because they have overlays that are concatenated on the end of the EXE file. So if the EXE file can't be read, the overlays can't be loaded.

3. You can make individual files read-only using the DOS attribute, and then deny the user the modify attribute privilege in that directory.

Using a combination of the three techniques above, you should be able to make a large percentage of the files on the server uninfectable (indeed, unchangeable without Supervisor intervention). This stops viruses infecting most of the executables on the server. Unfortunately, the important files on the server are the data, and you haven't protected those. The user has read/write access to the data (he needs it to do his job), and so the virus also has read/write access to the data. Deleting files is the least of our worries – consider that some virus damage routines consist of altering files. So how do we protect the data on the server? The only answer is to keep viruses off the workstation as well.

The next thing you can do, if your server is Novell, is run an anti-virus NLM (NetWare Loadable Module) on the server. This can check the files on the server and as they are passed to and from the workstations. It can also be used to prohibit the user from logging on unless he has his virus protection in place.

If your server is Lan Manager or Lan Server, you can run an OS/2 version of the anti-virus program on the server.

4 A brief history of viruses

1986-1987 – the prologue

It all started in 1986. Basit and Amjad realised that the boot sector of a floppy diskette contained executable code, and this code is run whenever you start up the computer with a diskette in drive A:. They realised that they could replace this code with their own program, that this could be a memory resident program, and that it could install a copy of itself on each floppy diskette that is accessed in any drive. The program copied itself – they called it a virus. But it only infected 360Kb floppy disks.

In 1987, the University of Delaware realised that they had this virus when they started seeing the label ' (c) Brain' on floppy diskettes. That's all it did – copy itself, and put a volume label on diskettes. This was also the first virus that was seen by S&S. A PC Support lady at a university phoned because she was seeing the volume label on a number of diskettes, and she thought it might be a virus, and because S&S was involved in data recovery from disks, thought we might be able to help. She sent us the virus, we analysed it, and that got S&S into the anti-virus business.

Meanwhile, also in 1986, a programmer called Ralf Burger realised that a file could be made to copy itself by attaching a copy of itself to other files. He wrote a demonstration of this effect, which he called ***Virdem.*** He distributed it at the Chaos Computer Club conference that December, where the theme was viruses. ***Virdem*** would infect any COM file; again the payload was pretty harmless.

This attracted so much interest that he was asked to write a book. Ralf hadn't thought of boot sector viruses like ***Brain,*** so his book doesn't even mention them. But by then, someone had started spreading a virus, in Vienna.

In 1987, Franz Swoboda became aware that a virus was being spread in a program called Charlie. He called it the Charlie virus. He made lots of noise about the virus (and got badly bitten as a result). At this point, there are two versions of the story – Burger claims that he got a copy of this virus from Swoboda, but Swoboda denies this. In any case, Burger obtained a copy, and gave it to Bernt Fix, who disassembled it (this was the first time anyone had disassembled a virus). Burger included the disassembly in his book, after patching out a couple of areas to make it less infectious and changing the payload. The normal payload of ***Vienna*** (or Charlie, as Swoboda called it) is to cause one file in eight to reboot the computer (the virus patches the first five bytes of the code); Burger (or maybe Fix) replaced this reboot code with five spaces. The effect was that patched files hung the computer, instead of rebooting. This isn't really an improvement.

Meanwhile, in the US, Fred Cohen had completed his doctoral dissertation which was on computer viruses. Dr Cohen proved that you cannot write a program that can, with 100% certainty, look at a file and decide whether it is a virus. Of course, no one ever thought that you could, but Cohen made good use of an existing mathematical theorem and earned a doctorate. He also did some experiments; he released a virus on a system, and discovered that it travelled further and faster than anyone had expected.

In 1987, Cohen was at Lehigh University, as was Ken van Wyk. So was the author of the ***Lehigh*** virus. ***Lehigh*** was an extremely unsuccessful virus – it never managed to spread outside its home world, because it could only infect COMMAND.COM and did a lot of damage to its host after only four replications. One of the rules is that a virus that quickly damages its host cannot survive. However, the ***Lehigh*** virus got a lot of publicity, and led to van Wyk setting up the Virus-L news group on Usenet. ***Lehigh*** was nasty. After four replications, it did an overwrite on the disk, hitting most of the File Allocation Table. But a virus that only infects COMMAND.COM isn't very infectious.

Meanwhile, in Tel Aviv, Israel, another programmer was experimenting. His first virus was called ***Suriv-01*** (virus spelled backwards). It was a memory resident virus, but it could infect any COM file (so could ***Virdem***, but ***Virdem*** wasn't TSR), whereas ***Lehigh*** could only infect COMMAND.COM. This is a much better infection strategy than the non-TSR strategy used by ***Vienna***, as it leads to files on all drives and all directories being infected. His second virus was called ***Suriv-02***, and that could infect only EXE files, but it was the first EXE infector in the world. His third attempt was called ***Suriv-03***, and it could handle COM and EXE files. His fourth effort escaped into the world, and became known as ***Jerusalem*** virus. Every Friday 13th, instead of infecting files that are run, it deletes them. But Friday 13ths are not common, so the virus is pretty inconspicuous most of the time. It avoids infecting COMMAND.COM, because in those days many people believed that this was the file to watch (see ***Lehigh***).

It looks as if it escaped rather than was released, because it plainly was not ready for release. The author decided to change the way that the virus detected itself in EXE files, and had made part of that change. There is redundant code from the ***Suriv*** viruses still in place, and what looks like debugging code. It was found in the Hebrew University of Jerusalem (hence the name) by Yisrael Radai.

While all this was going on, a young student at the University of Wellington, New Zealand, had found a very simple way to create a very effective virus. One time in eight, when booting from an infected floppy, it also displayed the message 'Your PC is now Stoned', hence the name of the virus.

The virus itself was just a few hundred bytes long, but because of its self-restraint and memory-resident replication, it became the most widespread virus in the world, accounting for over a quarter of outbreaks. It is very unlikely that ***Stoned*** virus will ever become rare. The virus spread rapidly, because of its inconspicuity (and because in those days, people were keeping a careful eye on COMMAND.COM because of ***Lehigh***).

In Italy, at the University of Turin, a programmer was writing another boot sector virus. This one put a bouncing ball up on the screen, if the disk was accessed exactly on the half hour. It became known as ***Italian*** virus, ***Ping Pong,*** or ***Bouncing Ball.*** But this virus had a major defect – it couldn't work on anything except an 8088 or 8086 computer because it uses an instruction that doesn't work on more advanced chips. As a result, this virus has almost died out (as has ***Brain,*** which can only infect 360Kb floppies, and which foolishly announces its presence via the volume label).

Back in the US, the ***Yale*** virus appeared. The ***Lehigh*** virus hadn't made it outside a small circle – neither did the Yale virus. This was another boot sector virus, but it only copied itself when you booted from an infected floppy, then put another floppy into continue the boot process. No subsequent diskette was infected, and if the boot-up continued from a hard disk there was no infection at all.

But also in 1987, a German programmer was writing a very competent virus, ***Cascade,*** so called after the falling letters display that it gave. ***Cascade*** used a new idea – most of the virus was encrypted, leaving only a small stub of code for decrypting the rest of the virus. The reason for this was not clear, but it certainly made it more difficult to repair infected files, and it restricted the choice of search string to the first couple of dozen bytes. This idea was later extended by Mark Washburn when he wrote the first polymorphic virus, ***1260*** (***Chameleon***). Washburn based ***Chameleon*** on a virus that he found in a book – the ***Vienna,*** published by Burger.

Cascade was supposed to look at the BIOS, and if it found an IBM copyright it would refrain from infecting. This part of the code didn't work. The author soon released another version of the virus, 1704 bytes long instead of 1701, to correct this bug. But the corrected version had a bug that meant that it still didn't detect IBM BIOSes.

Of these early viruses, only ***Stoned*** is common today.

1988 – the game begins

1988 was fairly quiet as far as virus writing went. Mostly, it was the year that anti-virus vendors started appearing, making a fuss about what was then only a potential problem, and not selling very much anti-virus software. The vendors were all small companies, selling their software for very low prices

($5 or $10 was common). Some of them were shareware, some were freeware. Occasionally some larger company tried to pop up, but no-one was paying serious cash to solve what was only a potential problem.

In some ways, that was a pity, because 1988 was a very virus-friendly year. It gave ***Stoned, Cascade*** and ***Jerusalem*** a chance to spread undetected, and to establish a pool of infected objects that will ensure that they never become rare.

It was in 1988 that IBM realised that it had to take viruses seriously. This was not because of the well-known Christmas tree worm, which was pretty easy to deal with. It was because IBM had an outbreak of ***Cascade*** at the Lehulpe site (in Belgium), and found itself in the embarrassing position of having to inform its customers that they might have become infected there. In fact, there was no real problem, but from this point on IBM took viruses very seriously indeed, and the High Integrity Computing Laboratory in Yorktown was given responsibility for the IBM research effort in this field.

1988 saw a few scattered, sporadic outbreaks of ***Brain, Italian, Stoned, Cascade*** and ***Jerusalem.*** It also saw the final arguments about whether viruses existed or not. Peter Norton, in an interview, said that they were an urban legend, like the crocodiles in the New York sewers, and one UK expert claimed that he had a proof that viruses were a figment of the imagination. In 1988, the real virus experts would debate with such people – after that year, real virus experts would simply walk away from anyone who had such absurd beliefs.

Each outbreak of a virus was dealt with on a case-by-case basis. Existing software was used to detect boot sector viruses (by inspecting the boot sector), and one-off software was written for dealing with outbreaks of ***Cascade*** and ***Jerusalem.***

In 1988, a virus called ***Virus-B*** was written. This is another virus that doesn't go memory resident, and it is a modification of another virus that deletes files on Friday 13th. When this virus is run, it displays 'WARNING!!!! THIS PROGRAM IS INFECTED WITH VIRUS-B! IT WILL INFECT EVERY .COM FILE IN THE CURRENT SUB DIRECTORY!'. A virus as obvious as that was clearly not written to spread. It was obviously written as a demonstration virus. Virus researchers are often asked for 'harmless viruses' or 'viruses for demonstration'; most researchers offer some alternative, such as an overhead foil, or a non-virus program that does a falling letters display. But it looks as if ***Virus-B*** was written with the intention of giving it away as a demonstration virus – hence the warning. And, indeed, we found that an American company was offering it to 'large corporations, universities and research organisations' on a special access basis.

At the end of 1988, a few things happened almost at once. The first was a big outbreak of ***Jerusalem*** at a large financial institution, which meant that dozens of people were tied up in doing a big clean-up for several days. The second was that a company called S&S did the first ever Virus Seminar that actually explained what a virus was and how it worked. The third thing was January, Friday 13th, which was actually in 1989, but logically belongs with the previous year..It was clear that we couldn't go out and help everyone with a virus. It was also clear that the financial institution, and the academic site, could easily handle a virus outbreak, but they didn't have the tools to do the job. All they needed was a decent virus detector, which was not available. So Dr. Alan Solomon wrote one, added some other tools that experience said might be useful, and created the first Anti-Virus Toolkit, which with some imagination, he called 'Dr Solomon's Anti-Virus Toolkit'.

In 1989, the first Friday 13th was in January. At the end of 1988, it was clear that ***Jerusalem*** was in Spain and the UK, at least, and was in academic as well as commercial sites. Because of the destructive payload in the virus, we felt that if we failed to send out some sort of warning, we would be negligent. But the media grabbed the ball and ran with it; the predictability of the trigger day, together with the feature of it being Friday 13th caught their imagination, and the first virus media circus was under way.

On the 13th of January, we had dozens of phone calls, mostly from the media wanting to know if the world had ended yet. But we also had calls from a large corporate site, a small vendor of PC hardware, and a couple of single users. We were invaded by TV cameras in droves, and had to schedule them carefully to avoid them tripping over each other. In the middle of all this, the PC Support person from the infected corporate arrived. The TV people wanted nothing better than a victim to film, but the corporate wanted anonymity. We pretended that he was just one of our staff. Also, at that time, British Rail contacted us – they also had an outbreak of ***Jerusalem***, and they went public on it. Later, they regretted that decision, because for a long time afterwards, their PC Support person was badgered by the media seeking interviews.

1989 – Datacrime

1989 was the year that things really started to move. The ***Fu Manchu*** virus (a modification of ***Jerusalem***) was sent anonymously to a virus researcher in the UK, and the ***405*** virus (a modification of the overwriting virus in the Burger book) was sent to another UK researcher. A third UK researcher wrote a virus and sent it to another UK researcher – in 1989, the UK was where it was all happening. But not quite all. In 1989, the Bulgarians started getting interested in viruses, and Russia was beginning to awaken.

In March of 1989, a minor event happened that was to trigger an avalanche. A new virus was written in Holland. A Dutchman calling himself Fred Vogel (a very common Dutch name) contacted Alan Solomon, and said that he had found this virus all over his hard disk. He also said that it was called ***Datacrime,*** and that he was worried that it would trigger on the 13th of the next month.

When the virus was disassembled, it was found that on any day after October 12th, it would trigger a low level format of cylinder zero of the hard disk, which would, on most hard disks, wipe out the File Allocation Table, and leave the user effectively without any data. It would also display the virus's name, ***Datacrime.*** A straightforward write-up of the effect of this virus was published, but it was another non-memory-resident virus, and so highly unlikely to spread.

However, the write-up was reprinted by a magazine, another magazine repeated the story, a third party embellished it a bit, and by June it was becoming an established fact that it would trigger on October 12th (not true, it triggers on any day after the 12th, until December 31st) and that it would low-level format the whole hard disk. In America, the press started calling it 'Columbus Day virus' (October 12th) and it was suggested that it had been written by Norwegian terrorists, angry because it was Columbus, not Eric the Red, who was attributed to discovering America.

Meanwhile, in Holland, the Dutch police were doing one of the things that police are supposed to do – crime prevention. ***Datacrime*** virus was obviously a crime, and the way to prevent it was to run a detector for it. So they commissioned a programmer to write a ***Datacrime*** detector, and offered it at Dutch police stations for $1. It sold really well. But it gave a number of false alarms, and it had to be recalled, and replaced with version 2. There were long queues outside the Dutch police stations, and lots of confusion about whether anyone actually had this virus (hardly anyone did, but the false alarms muddied the waters).

If the police take something seriously, it must be serious, right? So in July, large Dutch companies started asking IBM if viruses were a serious threat. ***Datacrime*** isn't, but there is a distinct possibility that a company could get ***Jerusalem, Cascade*** or ***Stoned*** (or ***Italian,*** in those days before 8088 computers became a rarity). 'So what is IBM doing about this threat', they asked?

IBM had internal-use-only anti-virus software. They used this to check incoming media, and to make sure that an accident like Lehulpe could never happen again. IBM had a problem – if they didn't offer this software to their customers, they could look very bad if on October 13th a lot of computers went down. The technical people knew that this wouldn't happen, but obviously they knew that someone, somewhere, might have important data

on a computer that would get hit by ***Datacrime.*** IBM had to make a decision about whether to release their software, and they had a very strict deadline to work to – October the 13th would be too late.

In September of 1989, IBM sent out version 1.0 of the IBM scanning software, together with a letter telling their customers what it was, and why they were sending it out. When you get a letter like that from IBM, and a disk, you would be pretty brave to take no notice, so a lot of large companies scanned a lot of computers, for the first time. Hardly anyone found ***Datacrime,*** but there were instances of the usual viruses.

October 13th fell on a Friday, so there was a double event – ***Jerusalem*** and ***Datacrime.*** In the US, ***Datacrime*** (Columbus Day) had been hyped out of all proportion for a virus that is as uninfective as this one, and it is highly likely that not a single user had the virus. In Europe (especially in Holland) there might have been a few, but not many.

In London, the Royal National Institute for the Blind announced that they'd been hit, and had lost large amounts of valuable research data and months of work. We investigated this particular incident, and the truth was that they had a very minor outbreak of ***Jerusalem,*** and a few easily replaced program files had been deleted. Four computers were infected. But the RNIB outbreak has passed into legend as a 'Great Disaster'. Actually, the RNIB took more damage from the invasion of the television and print media than from the virus.

1989 closed with the Aids Information Diskette. 20,000 copies of a diskette were mailed to users taken from mailing lists such as the one belonging to PC Business World. The diskette came with installation instructions (and a request for $189), and if you installed it, it created hidden directories and hidden files, and edited your AUTOEXEC.BAT so that one of these hidden files was run on each boot-up. This counted up to 90, and when it reached that number of boots the trojan would trigger. The trojan encrypted all the filenames on your hard disk, and gave them the hidden attribute, and it looked as if there was only one file on your hard disk, which was an invoice for $189 to be sent to PO Box 7, Panama.

The police investigated the incident, and this led to the arrest and extradition from the US of one Dr. Popp. He pleaded diminished competence, and was allowed to return to the US, but he was also tried in absentia in Italy, where he was sentenced to a prison term.

The main impact of the Aids diskette was a major flurry of publicity for malicious software (it wasn't a virus, but many people didn't care about the distinction). Also, a surprising number of people installed the software – PC Business World wrote a program to reverse the actions of the diskette, and made it available free of charge.

By the end of 1989, there were a couple of dozen viruses that we knew about, but we didn't know that in Bulgaria and Russia, big things were brewing.

1990 – the game gets more complex

By 1990, it was no longer a matter of running a couple of dozen search strings down each file. Mark Washburn had taken the ***Vienna*** virus, and created the first polymorphic virus from it. We didn't use that word at first, but the idea of his viruses (***1260, V2P1, V2P2*** and ***V2P6***) was that the whole virus would be variably encrypted, and there would be a decryptor at the start of the virus. But the decryptor could take a very wide number of forms, and in the first few viruses the longest possible search string was just two bytes long (***V2P6*** got this down to one byte). To detect this virus it was necessary to write an algorithm that would apply logical tests to the file, and decide whether the bytes it was looking at were one of the possible decryptors.

One consequence of this, was that some vendors couldn't do it. It isn't easy to write such an algorithm, and many vendors were, by this time, relying on search strings extracted by someone else. The three main sources of search strings were a newsletter called Virus Bulletin, the IBM scanner, and reverse engineering a competitor's product. But you can't detect a polymorphic virus this way (indeed, years after these viruses were published, many products are still incapable of detecting these viruses). Washburn also published his source code, which is now widely available. At the time, we thought that this would bring out a number of imitators; in practice, no-one seems to be using Washburn's code. However, plenty of virus authors are using his idea.

Another consequence of polymorphic viruses was an increase in the false alarm rate. If you write code to detect something that has as many possibilities as ***V2P6***, there is a chance that you will flag an innocent file, and that chance is much greater than with the sort of virus that you can find with a 24-byte scan string. A false alarm can be more hassle to the user than a real virus, as he will put all his anti-virus procedures into action.

Also in 1990 we saw a number of viruses coming out of Bulgaria, especially from someone who called himself 'Dark Avenger'. The ***Dark Avenger*** viruses introduced two new ideas. The first idea was the 'fast infector'; with these viruses, if the virus is in memory, then simply opening a file for reading triggers the virus infection. The entire hard disk is very soon infected. The second idea in this virus was that of subtle damage. ***Dark Avenger-1800*** occasionally overwrites a sector on the hard disk. If this isn't noticed for a period of time, the corrupted files are backed up, and when the backup is restored, the data is still no good. ***Dark Avenger*** targets backups, not just data. Other viruses came from the same source, such as the ***Number-of-the-Beast*** (stealth in a file virus) and ***Nomenklatura*** (with an even nastier payload than ***Dark Avenger***).

Also, Dark Avenger was more creative about distributing his viruses. He would upload them to BBSes, infecting shareware anti-virus programs, together with a documentation file that gave reassurance to anyone who checked the file size and checksums. He also uploaded his source code so that people could learn how to write viruses.

In 1990, another event happened in Bulgaria – the first virus exchange BBS (VX BBS). The idea was that if you uploaded a virus, you could download a virus, and if you uploaded a new virus, you were given full access. This, of course, encourages the creation of new viruses, and gets viruses into wider circulation. Also, the VX BBS offered source code, which makes the technology of writing a virus more widely available.

In the second half of 1990, ***The Whale*** appeared. ***Whale*** was a very large, and very complex, virus. It didn't do very much; mostly, it crashed the computer when you tried to run it. But it was an exercise in complexity and obfuscation, and it arrived in the virus researcher's hands like a crossword puzzle to be solved. Some virus researchers wasted weeks unravelling ***Whale***, although in practice you could detect it with a couple of dozen search strings, and you didn't really need to do any more, as the thing was too clumsy to work anyway. But because it was so large and complex, it achieved fame at the time.

At the end of 1990, the anti-virus people saw that they had to get more organised – they had to be at least as organised as the virus authors. So EICAR (European Institute for Computer Anti-virus Research) was born in Hamburg, in December 1990. This gave a very useful forum for the anti-virus researchers and vendors to meet and exchange ideas (and specimens), and to encourage the authorities to try to prosecute virus authors more vigorously. When EICAR was founded, there were about 150 viruses, and the Bulgarian 'virus factory' was in full swing.

1991 – product launches and polymorphism

In 1991, the virus problem was sufficiently interesting to attract the large marketing companies. Symantec launched Norton Anti Virus in December 1990, and Central Point launched CPAV in April 1991. This was soon followed by Xtree, Fifth Generation and a couple of others. Most of these companies were rebadging other companies' programs (nearly all Israeli). The big problem of 1991 was 'glut'. In December 1990, there were about 200-300 viruses; by December 1991 there were 1000 (there may have been even more written that year, because by February, we were counting 1300).

Glut means lots of viruses, and this causes a number of unpleasant problems. In every program, there must be various limitations. In particular, a scanner has to store search strings in memory, and under DOS, there is only 640Kb to use (and DOS, the network shell and the program's user interface might take half of that).

Another glut problem is that some scanners slow down in proportion to the number of viruses scanned for. Not many scanners work this way, but it certainly poses a problem for those that do.

A third glut problem comes with the analysis of viruses; this is necessary if you want to detect the virus reliably, to repair it, and if you want to know what it does. If it takes one researcher one day to disassemble one virus, then he can only do 250 per year. If it takes one hour, that figure becomes 2000 per year, but whatever the figure, more viruses means more work.

Glut also means many viruses that are similar to each other. This can lead to mis-identification, and therefore a wrong repair. Very few scanners attempt a complete virus identification, so this confusion about exactly which virus is being found, is very common.

Most of these viruses came from Eastern Europe and Russia – Russian virus production was in full swing. But another major source of new viruses was the virus exchange BBSes which were beginning to be seen all over the world.

Bulgaria pioneered the VX BBS, but a number of other countries quickly followed. Some shut down not long after they started up, but the Milan 'Italian Virus Research Laboratory' was where a virus author called Cracker Jack uploaded his viruses (which were plagiarised versions of the Bulgarian viruses). Germany had Gonorrhoea, Sweden had Demoralised Youth, America had Hellpit, UK had Dead On Arrival and Semaj. Some of these have now either closed down or gone underground, but they certainly contributed to the glut problem. With a VX BBS, all a virus author has to do is download some source code, make a few simple changes, then upload a new virus, which gives him access to all the other viruses on the board.

1991 was also the year that polymorphic viruses first made a major impact on users. Washburn had written ***1260*** and the ***V2*** series long before, but because these were based on ***Vienna*** they weren't infectious enough to spread. But in April of 1991, ***Tequila*** burst upon the world like a comet. It was written in Switzerland, and was not intended to spread. But it was stolen from the author by a friend, who planted it on his father's master disks. Father was a shareware vendor, and soon ***Tequila*** was very widespread.

Tequila uses full stealth when it installs itself on the partition sector, and in files it uses partial stealth, and is fully polymorphic. A full polymorphic virus is one for which no search string can be written down, even if you allow the use of wild cards. ***Tequila*** was the first polymorphic virus that was widespread. By May, the first few scanners were detecting it, but it was not until September that all the major scanners could detect it reliably. If you don't detect it reliably, then you miss, say, 1% of infected files. The virus starts another outbreak from these overlooked instances, and has to be put down again, but now there is that old 1%, plus another 1% of files that are infected but not detected. This can continue for as long as the user has patience, until eventually the hard disk contains nothing but files that the

scanner cannot detect. The user, thinks that although the virus comes back a number of times, it gradually infects fewer and fewer files, until now he has got rid of it completely (he thinks).

In September 1991, ***Maltese Amoeba*** spread through Europe – another polymorphic virus. By the end of the year, there were a few dozen polymorphic viruses. Each of these is classified as 'difficult', meaning it takes a virus researcher more than a few hours to do everything that needs to be done. Also, most products need some form of hard coding to detect the virus, which means program development, which means bugs, debugging, beta testing and quality control. Furthermore, although a normal virus won't slow down most scanners, a polymorphic virus might.

It was also in 1991 that Dark Avenger announced the first virus 'vapourware'. He threatened a virus that had 4,000,000,000 different forms. In January 1992, this virus appeared, but it wasn't a virus.

1992 – a very busy year

January 1992 saw the ***Self Mutating Engine (MtE)*** from Dark Avenger. At first, all we saw was a virus that we named ***Dedicated,*** but shortly after that, we saw the ***MtE.*** This came as an OBJ file, plus the source code for a simple virus, and instructions on how to link the OBJ file to a virus to give you a full polymorphic virus. Immediately, virus researchers set to work on detectors for it. Most companies did this in two stages. In some outfits, stage one was look at it and shudder, stage two was ignore it and hope it goes away. But at the better R&D sites, stage one was usually a detector that found between 90 and 99% of instances, and was shipped very quickly, and stage two was a detector that found 100%. At first, it was expected that there would be lots and lots of viruses using the ***MtE,*** because it was fairly easy to use this to make your virus hard to find. But the virus authors quickly realised that a scanner that detected one ***MtE*** virus would detect all ***MtE*** viruses fairly easily. So very few virus authors have taken advantage of the engine.

This was followed by Dark Avenger's ***Commander Bomber.*** Before ***Commander Bomber,*** you could very easily predict where in the file the virus would be. Many products take advantage of this predictability to run fast; some only scan the top and tail of the file, and some just scan the one place in the file that the virus must occupy if it is there at all. ***Commander Bomber*** transforms this, and so products either have to scan the entire file or else they have to locate the virus by following the code.

Another virus that came out at about that time was ***Starship. Starship*** is a fully polymorphic virus (to defeat scanners), with a few neat anti-debugging tricks, and it also aims to defeat checksummers with a very simple trick. Checksumming programs aim to detect a virus by the fact that it has to change executable code in order to replicate. ***Starship*** only infects files as they are copied from the hard disk to the floppy. So files on the hard disk

never change. But the copy on the floppy disk is infected, and if you then copy that on to a new hard disk, and tell the checksummer on the new machine about this new file, the checksummer will happily accept it, and never report any changes. ***Starship*** also installs itself on the hard disk, but without changing executable code. It changes the partition data, making a new partition as the boot partition. No code is changed, but the new partition contains the virus code, and this is run before it passes control on to the original boot partition.

Michelangelo

Probably the greatest event of 1992 was the great ***Michelangelo*** scare. One of the American anti-virus vendors forecast that five million computers would go down on March the 6th, and many other US vendors climbed on to the bandwagon. PC users went into a purchasing frenzy, as the media whipped up the hype. On March the 6th, only between 5,000 and 10,000 machines went down, and naturally the US vendors that had been hyping the problem put this down to their timely and accurate warning. We'll probably never know how many people had ***Michelangelo,*** but certainly in the days leading up to March the 6th many computers were checked for viruses. After March 6th, there were many discredited 'experts' around.

In August 1992, we saw the first serious virus authoring packages. First the VCL (Virus Creation Laboratory) from Nowhere Man, and then Dark Angel's Phalcon/Skism Mass-Produced Code Generator. These packages made it possible for anyone who could use a computer to write a virus. Within twelve months, dozens of viruses had been created using these tools.

Towards the end of 1992, a new virus writing group called ARCV (Association of Really Cruel Viruses) had appeared in England – within a couple of months, the Computer Crime Unit of New Scotland Yard had tracked them down and arrested them, with considerable help from the anti-virus community. ARCV flourished for about three months, during which they wrote a few dozen viruses and attracted a few members.

Another happening of 1992 was the appearance of people selling (or trying to sell) virus collections. To be more precise, these were collections of files, some of which were viruses, and many of which were assorted harmless files. In America, John Buchanan offered his collection of a few thousand files for $100 per copy, and in Europe, The Virus Clinic Unit offered various options from £25. The Virus Clinic was raided by the Computer Crime Unit after its first (and only) advert in Micro Computer Mart.

1993 – polymorphic viruses and engines

Early in 1993, XTREE announced that they were quitting the anti-virus business. This was the first time a major company had given up the struggle.

Also early in 1993, a new virus writing group appeared in Holland, called Trident. The main Trident author, Masouf Khafir, wrote a polymorphic engine called the ***Trident Polymorphic Engine,*** and released a virus that used it called ***GIRAFE.*** This was followed by updated versions of ***TPE.*** The ***TPE*** is much more difficult to detect reliably than the ***MtE,*** and very difficult to avoid false alarming on.

Khafir also released the first virus that worked according to a principle first described by Fred Cohen. The ***Cruncher*** virus was a compression virus that automatically added itself to files in order to auto-install on as many computers as possible.

Meanwhile, Nowhere Man of the Nuke group had been busy. Early in 1993, he released the ***Nuke Encryption Device (NED).*** This was another mutator that was more tricky than ***MtE.*** A virus called ***Itshard*** soon followed.

Phalcon/Skism was not to be left out. Dark Angel released ***DAME (Dark Angel's Multiple Encryptor)*** in an issue of 40hex: a virus called ***Trigger*** uses this. Trident released version 1.4 of ***TPE*** (again, this is more complex and difficult than previous versions) and released a virus called ***Bosnia*** that uses it.

Soon after that, Lucifer Messiah, of Anarkick Systems had taken version 1.4 of ***TPE*** and written a virus ***POETCODE,*** using a modified version of this engine (1.4b).

Also early in the year another highly polymorphic virus appeared called ***Tremor.*** This rocketed to stardom when it got included in a German TV broadcast of software (received through a decoder). The infected file was PKUNZIP.EXE, which most recipients used to decompress the files they received.

In the middle of 1993, the Trident group got a boost when Dark Ray and John Tardy joined the group. Tardy has released a fully polymorphic virus in 444 bytes, and we can expect more difficult things from Trident.

The main bad news of 1993 was the emergence of an increasing number of virus authoring packages and polymorphic engines, which make it easier to write viruses that scanners find difficult to detect.

Also in 1993, more significant anti-virus companies disappeared – Certus (whose products included Novi) was taken over by a competitor. Fifth Generation, whose product was called Untouchable, also disappeared.

There was some good news, though. S&S International received the Queen's Award for Technological Achievement. This was awarded for the virus description language, VIRTRAN which is at the heart of **FindVirus** and **VirusGuard.**

The generic decryption engine

The ongoing glut of viruses written using the packages presented a major problem for the anti-virus authors who were already hard pressed. It became necessary to mechanise the analysis.

The solution was the GDE (Generic Decryption Engine), which decrypts the code of a suspect file, leading to a firm decision whether it is a virus or not. This eliminates the danger of giving false alarms on such viruses – once the virus is decrypted, it is easy to make a positive identification of the virus.

1994

In April of 1994, Central Point Software ceased to exist. Central Point was one of the major players in the anti-virus market with their CPAV product.

More polymorphic engines and viruses appeared, such as ***SMEG,*** which was released into the wild by the author as ***Smeg.Pathogen*** and ***Smeg.Queeg.*** Because these were viruses that appeared in the wild so quickly after they came into existence, they have been an interesting test of the speed at which anti-virus companies can react.

1995

On the 26th May 1995, Chrisopher Pile, 26, of Plymouth in England, was convicted under the Computer Misuse Act in connection with the ***Smeg*** viruses.

The future

There will be more viruses – that's an easy prediction. How many more is a difficult call, but over the last five years the number of viruses has been doubling every nine months. This surely must slow down. There were 3700 viruses at the end of 1993, 6000 at the end of 1994, and we expect 7000 by the end of 1995.

The glut problem will continue, and could get quickly worse. Whenever a group of serious anti-virus researchers meets, we find an empty room, hang 'Closed for cleaning' on the door, and frighten each other with 'nightmare scenarios'. Some of the older nightmare scenarios have already come true, others have not, but remain possibilities. The biggest nightmare for all anti-virus people is glut. There are only about 10 or 15 first class anti-virus people in the world, and most of the anti-virus companies have just one of these people (some have none). It would be difficult to create more, as the learning curve is very steep. The first time you disassemble something like ***Jerusalem*** virus, it takes a week. After you've done a few hundred viruses, you could whip through something as simple as ***Jerusalem*** in 15 minutes.

The polymorphic viruses will get more numerous, and more complex. The need to detect them all will be a serious problem for anti-virus packages without GDE capability. They are a much bigger problem than the stealth viruses, because stealth is aimed at checksummers, but polymorphism is aimed at scanners, which are what most people are using. And each polymorphic virus will be a source of false alarms, and will cause the researchers much more work than the normal viruses.

Scanners will get larger – more code will be needed because more viruses will need hard coding to scan for them. The databases that scanners use will get larger; each new virus needs to be detected, identified and repaired. Loading the databases will take longer, and some programs will have memory shortage problems.

As Windows becomes more popular, people will be increasingly reluctant to run scanners under DOS. But if you are running Windows, you have run software on the hard disk, and if one of the things you've run is infected by a virus, you have a virus in memory. If there is a virus in memory, you cannot trust what the computer is saying – it could be a stealth virus. Windows will make anti-virus software less secure.

The R&D effort to keep scanners up-to-date will continue to increase. Some companies won't be able to do it, and will decide that scanning is outdated technology and try to rely on checksumming. Other companies will licence scanners from one of the few companies that still maintain adequate R&D (we've already started seeing some of this). Some companies will decide that the anti-virus business isn't as profitable as they had thought, and will abandon their anti-virus product and go back to their core business.

Users will get a lot more relaxed about viruses. We've long since passed the stage where a virus is regarded as a loathsome disease, to be kept secret. But we're increasingly seeing people who regard a virus on their system with about the same degree of casualness as a bit of fluff on their jacket. Sure, they'll wipe it off, but there's not real need to worry about it happening again. This is perhaps a bit too relaxed an attitude, but what can you expect if a user keeps on getting hit by viruses, and nothing terrible ever seems to result.

Anti-virus products will mature a lot. Those without any kind of decent user interface will have a hard time competing against the pretty ones. Those with a long run time will be rejected in favour of those that run in seconds. Exactly which viruses are detected will have far less emphasis (it is very difficult for users to swallow claims about so many thousands of viruses) than the ease of use of the product, and the amount of impact it has on the usability of the computer.

New products will keep arriving as each company invents the product that makes all previous products obsolete. Sometimes the magic ingredient will be software (AI, neural nets, whatever is the latest buzzword) and sometimes it will be hardware (which can never be infected, except that that isn't the problem). These products will burst on a startled world in a blaze of publicity, and vanish without trace when users find that installing them makes their computer unusable, or else it doesn't find any viruses, or both. But new ones will come along to take their place.

Gradually, people will trade up from DOS to whatever takes its place – OS/2, Windows 95, Windows-NT or UNIX, and the DOS virus will become as irrelevant as CPM. Except that DOS will still be around 10 years from now. Operating systems are being promoted as secure, but the computers they are installed on are not secure against viruses, any more than they are secure against theft. It is extraordinarily difficult to write an operating system that is virus-proof without it also being useless for most other purposes.

Some computers are already being built with ingrained resistance to viruses. Some brands of computer are already immune to boot sector viruses, provided you make a simple choice in the CMOS setup (don't boot from the floppy). Right now, very few users are being told that these computers can be set up that way, but people are gradually finding out for themselves. This doesn't solve the virus problem, but anything that makes the world a difficult place for viruses must be a help.

The virus problem will be with us for many years to come. It isn't the dramatic, world-shaking kind of problem that ***Michelangelo*** was made out to be; nor is it the fluff-on-your-jacket kind of problem. But as long as people have problems with computers, other people will be offering solutions for those problems.

5 Mechanisms of stealth

For a virus to be a virus, all it needs to do is copy itself. But to be a successful virus, it needs to be as inconspicuous as possible. Like a mouse, its main defence is that you don't know that it's there, because as soon as you spot it you'll swat it.

The generic term for the attempt to remain inconspicuous is stealth, but there are various degrees of stealth and various mechanisms for achieving this. Overall, we have been watching an increasing trend in this direction, for reasons we shall discuss.

Some technical information is given in this article. Be assured that this is not of use to virus authors, as it is all published in such standard reference manuals as the MS-DOS Encyclopaedia, published by Microsoft Press.

Some viruses are highly visible; for example the Burger viruses overwrite the beginning of the file that they infect, the program no longer functions and the user immediately notices that. There is absolutely no way that you can fail to notice an overwriting virus. We call this negative stealth, level -1. About 10% of viruses have negative stealth, and the obvious question is why? The reason must be that there is a segment of virus authors who really don't care about writing a virus that actually is survivable; all they want is the nice warm feeling that comes with being able to boast that you've written a virus. Boot sector viruses cannot have negative stealth – if they didn't pass on control to the original boot sector, the computer would not boot up at all.

The next level up is really necessary in order for the virus to spread at all. The original program must still run, or substantially so. This is done by adding the virus to the file, yet preserving all the necessary information for the program still to run, and for the virus to execute in addition to the original program. About 90% of viruses do this. We call this level 0 stealth. But if the virus does no more than this, it will be only moderately noticeable for the following reason: people don't look at time stamps.

Just in case they do (many magazines advocate this as an anti-virus measure), most viruses implement level 1, or elementary, stealth.

1. If date and time are not preserved during the infection, an increasing number of programs will have a current time stamp. This might be noticed by an alert user, and is certainly visible if you look out for it. It is avoided by using interrupt 21h, function 57h, although there are some viruses that use lower level methods to preserve date and time.

2. If a virus uses DOS writes to add itself to the file, and the disk is write-protected, DOS will give a critical error 'Abort, Retry, Fail'. This will be noticed – the user may ask why the disk is being written to when all he did was try to run a program. Again, it would need an alert user to spot this, and anyway write-protected media don't get used very

much. It is fairly easy to avoid this problem; the critical error comes to you via interrupt 24h, and it can be replaced temporarily with a small routine that does nothing at all. Boot sector viruses don't have to do anything about the above issues.

A virus that deals with the two problems above, we would call stealth level 1, or elementary stealth. In addition, to qualify for this level, the virus must do nothing flashy to call attention to itself. For example, the ***Diamond (V1024)*** virus displays every hour, on the hour. A multicoloured diamond pops up on the screen, shatters into diamond fragments which then dance around the screen, gradually clearing it. If you don't notice that, you need new glasses, and you are bound to twig that something odd is going on.

At stealth level 2, intermediate stealth, it starts getting more interesting. Below that level, the virus can be seen with the naked eye, as it were. In the case of a file virus, you could see the difference in file size, or in the case of a boot sector virus you would see a peculiar boot sector. It is possible to conceal the increase in file size, and this can be done in a number of ways. The most obvious way is not to have an increase in file size in the first place. The ***Zero-hunt*** virus looks for a block of contiguous zeros in the file, and if it finds this it overwrites that part of the file with itself. The file, therefore, does not grow at all. When the infected program runs, the virus runs first, and after going memory resident it overwrites the memory image of the file with zeros so that the program will run completely normally. The ***Rat*** uses a similar technique, but only works in EXE files, where it looks for the block of zeros that many compilers put at the start of the EXE file just after the header.

For most people, the only way they inspect file sizes is with a DIR command. DIR uses interrupt 21h, functions 11h and 12h. If the virus intercepts interrupt 21h and traps these functions, it can subtract the virus's length from the value returned, and pass this fake value on to any calling program. So DIR looks normal. ***Zero-Eater*** (also called ***Zero-bug***) uses this method.

There is another way to find out file size; interrupt 21h functions 4eh and 4fh. These are the handle equivalents of 11h and 12h, and some of the programs that act as a user shell for DOS use these calls to find out file sizes. Also, if an anti-virus program is checking on file sizes, it probably uses these functions as they are easier on the programmer than 11h and 12h. The virus can trap and fake these calls also.

A third way to find out file size is interrupt 21h function 42h subfunction 2. This is Seek to end of file, and the file size is returned in the registers. A sneaky anti-virus program might use this call to determine the file size, but there are sneaky viruses that do their subtraction on this also, such as ***Tequila.*** Of course, you can avoid such tricks by cold-booting from a known clean DOS diskette which is what we tell users to do. We also know that the number of people who actually do this before running their anti-virus software can be counted on the fingers of one hand. We have to assume that people don't do

as instructed in the manual because a lot of them didn't read the manual, and a lot of those that did read the manual have decided that it isn't necessary to do what they've been told.

One problem with the three methods above is that the virus must be in memory for the stealth to operate, and maybe the virus hasn't been run yet, or maybe the user has cold-booted from a clean DOS diskette. The next way to avoid the apparent growth in file size is to increase the file in size, but not let the directory entry reflect this. The ***Number of the Beast*** virus is 512 bytes long, and replaces the first sector of the file with itself. But it needs that original sector, so it stores it after the end of the file, in the space between the end of the file and the end of the cluster. Most hard disks have 2Kb clusters, so about 75% of files will have the necessary space available. A problem with this approach is that when you copy that file on to a floppy disk, the cluster size will be 1Kb at most, and high capacity floppies have a cluster size of 1/2Kb. When you copy an infected file on to floppies the virus will be copied, but not all of the original program. ***Number of the Beast*** has been seen in the wild in Western Europe, but not yet in the USA.

V1963 virus (and ***V1963B***, also called ***Necrophilia***) needs 1963 bytes, so this technique would not be very successful. Instead, it adds one cluster to the FAT chain and uses that to store the first 1963 bytes of the original file. The directory entry is left unchanged so that even if the virus is not in memory the file size does not look suspicious.

In the case of boot sector viruses, for the virus to be intermediate stealth it would have to show the original boot sector whenever a request is made to read the boot sector. ***Brain*** was the first virus that did this. But the fact that it readily puts a volume label on the diskette '(c) Brain', plus the noticeable 3Kb in bad sectors on the diskette, really disqualifies it from being intermediate stealth.

Most of the so-called stealth viruses in many virus catalogues are actually intermediate stealth. Very few intermediate stealth viruses are successful, though. Since very few people go looking for viruses, the benefit of intermediate stealth over elementary stealth is not really as great as it would seem. To reap real benefits in invisibility it is necessary to go to advanced stealth. In advanced stealth, the virus aims to be invisible to anti-virus programs. But first, we shall cover a few assorted stealth tricks.

Assorted stealth techniques

Certain anti-virus programs work by intercepting the interrupts and blocking naughty attempts, such as the attempt to write to COM or EXE files. If such a program is in memory, it is clearly a good idea to disable it before it infects anything. One well-known example of such a program has, in some versions, provided a convenient way for users to do this, so that a user wishing to

perform some action that would be flagged can do so without raising a false alarm. Some viruses, such as ***Eight Tunes***, detect this product by using its own 'Are you there?' call.

Another technique that we see sometimes was prompted by the fact that many scanning programs do a self-check before running, and if there is any change to the file they report this. This would mean that a new virus might be detected in this way. So some of the viruses refrain from infecting such programs; one common way is to look for the letters SC or SCAN at the beginning, or alternatively anywhere, in the filename. Another string that they avoid is a file with TEST in the name. You might consider renaming your scanner, although it might object to this.

Viruses that stealth the file size often leave an inconsistency between the size according to the directory entry and the number of elements in the FAT chain. When CHKDSK is run, it will report these inconsistencies, and CHKDSK is a program that is often run when problems are suspected. To avoid the suspicious report by CHKDSK, at least one virus checks the name of the program being run, and if it is CHKDSK, the file size stealth is disabled.

Advanced stealth

A virus that uses advanced stealth is aiming to conceal its existence even from anti-virus software. The best known example of this is ***Frodo***, also known as ***4096***, ***4K*** and ***IDF***. ***Frodo*** is much misunderstood. We've seen reports that it disinfects itself when read, which is a rather curious way of describing what it actually does. In fact, it traps interrupt 21h, and when any file-related operations are performed it swings into action. When any program uses DOS to read, write, seek or whatever in the file, ***Frodo*** works out what that DOS call would have seen if the file had not been infected, and returns that information for DOS to present to the calling program. The result is that with ***Frodo*** in memory, even if you do a byte-by-byte comparison between an infected file and a clean copy (which would perhaps be on a write-protected floppy disk), the comparison would report no difference. ***Frodo*** marks files by adding 100 years to the date stamp (hence the alias ***100 years***, and even the existence of this is concealed). As a result, it is difficult to notice that ***Frodo*** is present, and tricky to get rid of it.

It has a neat way of concealing itself in memory, too. Most programs that go memory-resident and capture an interrupt do so by changing the entry in the interrupt vector table. As a result, some people have guessed that this is the only way to do this. But ***Frodo*** avoids this method to fool programs that check for changes in the IVT. Instead, ***Frodo*** patches the first five bytes of the interrupt handler with a jump to the ***Frodo*** code. After the ***Frodo*** code is run, it then re-patches the original DOS kernel back to what it was before, and jumps to it.

Number of the Beast (so called because of the 666 in the code) is exactly 512 bytes long (there are about a dozen versions of it now). It is also an advanced stealth virus, but it does this trick by manipulating the system file tables inside DOS. The 512 bytes of the virus are very tightly coded – it looks like a Swiss watch, although perhaps that should be a Bulgarian watch. If there is any attempt to read the first 512 bytes of an infected file while the virus is in memory, it fetches the original 512 bytes that it has placed after the end of the file, and presents those instead. Again, DOS Compare and cryptographic checksummers are fooled into thinking that the file is unchanged from the original.

It also has a neat way of hiding in memory. It needs precisely 512 bytes of storage, and it gets this by taking the first DOS buffer, and convincing DOS that the second buffer is actually the first. Thus, most memory mappers will not recognise this 512 byte hole in memory, or else think that it is part of DOS.

Amongst boot sector viruses, ***Joshi*** and ***EDV*** use advanced stealth techniques. With either of these viruses, if the virus is in memory and you look at the sector that contains the virus code, the virus redirects the read to where it put the sector that it replaced, so that anti-virus software sees nothing amiss. ***EDV*** has some additional tricks. If you look at the place where it parked the sector it replaced, at cylinder 39, head 1 sector 8, the virus returns an unreadable sector error, so that you do not see a boot sector in such an unusual place. And when the virus goes memory-resident, it first tries to use memory above 640Kb, if there is RAM up there, so that memory mappers don't see it.

Joshi will survive a Ctrl Alt Del. Most people think that Ctrl Alt Del triggers a reboot; actually it is just another keystroke that can be replaced by replacing interrupt 9. This trick of ***Joshi***'s has allowed it to survive clean-up operations by people who think that all you have to do is reboot and low-level format hard disks – not only is this overkill, but also it doesn't necessarily do the job, unless you do the right things in the right order.

6 Polymorphic viruses

The main enemy of viruses, is the scanner. This is because this is the only tool that many people use (indeed, many people seem to believe that it is the only possible tool). So the virus authors have developed ways of concealing the existence of the virus from scanners, or at least making it more difficult to detect them this way.

Perhaps the first virus that started to do this, was ***Cascade***. Most of the virus is encrypted using two variable encryption keys. The only constant part of the virus is the decryptor/loader, which is a couple of dozen bytes of code that decrypts the rest of the virus so that it can run. This means that the designer of the scanner has only a couple of dozen bytes from which to choose the search string, and there is a lovely and obvious sequence to choose – 141$Flu. In the early days, many scanners chose this sequence, but failed to encrypt the search string in the scanner itself. As a result, scanners would find this string in each other, and give false alarms. These days, nearly every scanner encrypts all its search strings to avoid this problem, although there are still a few that don't, or which fail to clear them from memory after running, which leads to memory false alarms. Having only a few dozen bytes which are not encrypted in ***Cascade*** aggravates this problem.

The next step was when the virus authors started putting some variable bytes in the middle of the decryptor/loader. These bytes do nothing of significance, so can be any valid instruction, but this means that the scanner has to implement wildcard searches which adds some complexity to the program, although not a great deal. ***Phoenix, Evil, Proud*** and ***Virus101*** use this technique.

What followed was to make the number of non-significant instructions variable. To do this, there needs to be a random number generator in the virus to choose the non-significant instruction, and to choose the number of these instructions to be used. At this point, we begin to talk about a code generator in the body of the virus to generate different randomised decryptor/loaders. The ***Simulate*** virus uses this technique. It means that, putting on the virus researcher's white hat, we have to implement a search engine that is capable of accepting a wildcard which represents a variable number of bytes, although within certain limits. What are these limits? We need to know, because if we have, say, six three-byte search strings and allow these to occur within 64Kb of file, the probability of a false alarm is much greater than if we specify that they must all occur within 100 bytes. But until we have disassembled, analysed and understood the virus, we cannot make this prediction.

Then came the realisation that in many code sequences the exact order of the instructions doesn't affect the outcome. For example, if you load the AX register and then the CX register, the upshot is the same as if you load CX and then AX. So, putting on the virus author's black hat, if you write the code

generator to randomise the order of these instructions it makes it even harder to search for the virus. With the virus researcher's white hat on, either you have to give the search engine a great many search strings, or else you need some way to tell the scanner that within certain limits, the order of finding these fragments doesn't matter. Again, you have to disassemble and understand the virus to be able to predict the limits of the code generator. Also, the search engine is more complex again. ***Maltese Amoeba*** (also known as ***Irish***) uses this technique, which is why it is tricky to scan for accurately. Putting on the black hat again, the next step is to realise that there are many completely different code sequences that accomplish the same end.

For example, to copy the CS register into the DS register, you can do:

```
Push CS
Pop  DS
```

or

```
Mov AX, CS
Mov DS, AX
```

And so on. Again, the code generator can implement this; ***Tequila*** uses this method. Another trick is to realise that many of the registers on the 8088 can be used interchangeably for each other. So, instead of using AX to contain the decryption key, you can use DX, DI or SI, for example. Changing the register used changes one of the bytes in the decryption routine. The Washburn viruses ***1260, V2P1, V2P2, V2P6*** and ***V2P6Z*** use these techniques. In the ***1260*** virus the longest available search string is two bytes long, there are not many of them, and they occur in many different orders. ***V2P2*** is the same, and the number of bytes added to the original file is a variable; and in ***V2P6*** the longest possible search string is one byte long, and there are about half a dozen of these constant bytes which can occur in many different positions and in many different orders. The source codes of these viruses are floating around on the virus exchange BBSes, so anyone who wants to learn the technique can do so. Where the source codes are not available, there are disassemblies that you can download.

Putting on our white hat, how do you scan for such a virus? With great difficulty. Again, you have to disassemble, analyse and understand the code generator in the virus, and this might not be as easy as it sounds. But once you've done that, you can determine the relationships between the bytes (rules like, if the byte at offset 14 is a 67 then the byte at offset 19 must be a 73). And, finally, you can write a subroutine that can be linked into the software which can detect the virus in all its instances. But now we are talking about hard-coding the scan, as opposed to using search strings, which is more difficult and bug-prone. If you make the smallest mistake, you will either falsely accuse innocent files of harbouring the virus, or else fail to detect

one or more instances of the virus, which means that the virus survives the clean-up. Furthermore, if you are using published search strings, forget it – you can't publish a search string for these viruses.

Each virus that uses such a sophisticated decryptor/loader causes an immense amount of work for the scanner vendor, and we are beginning to see some of the vendors give up. This, of course, is another encouragement to the virus authors to use such techniques. If WonderScan (with apologies if there really is such a product) fails to detect any viruses that fall into this category, then any virus author that wants his virus to spread unimpeded only has to use a complex code generator of this kind to ensure that his virus spreads widely. However, many vendors are still staying with the game so far.

So let's raise the stakes some more. Since it is necessary for the virus researcher to disassemble, analyse and understand the virus code generator, the virus authors can make it more difficult for them to do so. This technique is used in ***Virus-101***; some of the code is written in a very obscure way, and uses features of the 8088 such as segment wraparound. Another technique is to make stepping through the code more difficult; one virus uses the 8088 pipeline, so that if you step through the code the computer reboots, but if you run the virus, that instruction is a simple jump to the next instruction. That isn't a problem; nor is the technique of disabling the keyboard as you step through the code, leaving you with a dead computer that you have to reboot.

The ***1260***, and the ***V2*** series use another method. Under the first layer of encryption there is a second layer. A few dozen of the bytes in the virus are encrypted with another encryption routine, such that if you simply disassemble after the first decryption the important parts of the virus make no sense. So you have to deal with the second layer of decryption, and you cannot do that by simply stepping through the code with Debug.

The way that Debug (and other debuggers) work is by putting a single-byte interrupt, interrupt 3, 0cch, into the code, saving the byte that used to be there. When the program reaches that point, the int 3 is executed, which stops the execution and triggers Debug's display. Another method that Debug uses is to put the processor into single step mode, and then every instruction executed also causes an interrupt 1, which can be programmed to do whatever is required, such as for example display the contents of the registers. Debug, therefore, needs to use interrupts 1 and 3. ***1260*** and the ***V2*** series use these interrupts to do the second layer of decryption. ***Tenbytes*** does the same, and the ***Fichv*** series from France uses interrupt 1 and interrupt 3, with a variable key sequence.

This means that you cannot single step through the virus. Every so often in the ***V2*** series there is a 0cch instruction in the virus, which calls interrupt 3 and interrupt 1 to decrypt the next two bytes using one as the key and the other as the byte to decrypt. But you can't write a program to automatically do the decryption because there are also dummy 0cch bytes that don't get

executed, so don't decrypt the following bytes. So if you write a program to treat each 0cch byte that way, you'll scramble those parts of the program as well as decrypting the parts that need decrypting. The virus author has raised the ante; to scan for the virus, you must understand the code generator, and to do that you have to disassemble the virus, which means that you have to break through the obfuscation. It is all possible, but it all takes time.

When one of our researchers disassembled ***Fish6***, he said that it took two weeks to do the virus, and another two weeks to uncross his eyes. Disassembling ***Whale*** is like doing a Listener crossword puzzle. If you ever get cast away on a desert island with a PC and Debug, and you get to choose one virus to take with you for entertainment, make it ***Whale***. Even a year after it first came out, the majority of scanner products are not able to detect all the faces that it can present to the world; this makes ***Whale*** quite a good test of companies' R&D in the field. Fortunately, ***Whale*** is incapable of working in a real environment, but there is always the possibility of Son of Whale. The technique of extreme obfuscation is sometimes called armouring, but it is a very standard thing in the copy protection field, where the copy protection vendors are keen that would-be pirates should not be able to understand their code.

Having discussed the theory of stealth, let's look at a real example, and the impact of it. The ***Tequila*** virus is quite common in Europe, and it has now just started to appear in the US. It was written in Switzerland, and a friend of the virus author planted it on the distribution disks of a shareware vendor. This gave it a good start in life.

When you run an infected EXE program, it installs itself on the partition sector of the hard disk. To do this, it uses another stealth technique called tunnelling. In the case of ***Tequila***, it puts the processor into single step mode, and calls interrupt 13h to reset the disk. But on every instruction, interrupt 1 is called, and ***Tequila*** has reprogrammed that to look at the location in memory that it is being called from. When it finds that it is being called from the firmware, it stores that address, and switches off the single step. Now ***Tequila*** knows the address of the hard disk controller firmware, and any program that is supposed to be blocking attempts to write to the hard disk via the interrupts is very easily evaded by doing a far call to the firmware. And ***Tequila*** installs itself on the partition sector.

Next time the computer starts up, the partition sector is run, and this happens before any anti-virus software can be run. This installs the virus into memory, and ***Tequila*** then stealths the partition so that any anti-virus software that examines the partition sees what was there before ***Tequila*** came along.

Now ***Tequila*** can start infecting files. It has a complex code generator in the body of the virus, so that the decryptor/loader of the rest of the code is very variable. There are a few two-byte strings you can scan for, and some one-byte strings that are reliably there. But some scanners have difficulty detecting all instances of the virus, and some scanners give false alarms on some innocent files because of the difficulty in doing it right.

The virus adds 2468 bytes to each infected file. But with the virus in memory, the growth in file size is concealed from programs that ask DOS for this information. So the virus is quite difficult to see, and easily gets copied onto diskettes and passed on.

The main outcome of the virus is a kind of Mandlebrot display in block graphics, three months after installing the virus on the hard disk. The main way that people notice the virus is when some program is incompatible with the virus; Windows is an example of this.

The future

Most of the viruses that we see are noise viruses; yet another version of ***Vienna, Burger*** or ***Jerusalem.*** But some of the virus authors are writing viruses that are designed to be difficult to detect, and survival of the fittest will of course ensure that these are the viruses that are most likely to become common in the longer run. When everyone is running the kind of simple scanner that can detect ***Jerusalem*** and ***Stoned,*** the only viruses that will spread will be the ones that make good use of polymorphism techniques. Polymorphism, therefore, is going to be increasingly important in the future. The consequence of this is that there will be more and more viruses that are difficult to deal with from the point of view of the virus researcher. From the point of view of the user, there will be more and more false alarms as scanners mistake innocent files for some of the results of the sophisticated code generators. Also, there will be an increasing number of situations where the scanner in use is not capable of detecting the virus, not because the scanner has not yet been upgraded to deal with a new virus, but because it is simply too much work for the vendor to keep up with the flood of new, and difficult viruses.

7 PC Viruses

The virus naming problem

When an anti-virus researcher finds a new virus, he wants to upgrade his software to detect it right away. But when his software finds the virus, it has to call it something. What name should he give it?

Whatever he decides to call it, he can be quite sure that three other anti-virus researchers are working on the same virus at the same time he is, and that they are each also giving it a name, and very often none of them are picking the same name. Viruses seldom come with a name conveniently attached. A few do have an obvious name enclosed in the virus by the virus author, but there is some reluctance to use such a name even in the few cases where it exists, because it tends to encourage and gratify the author. Still, whenever there is any text in a virus, it is likely that part of it will become the virus's name. This is how ***Stoned*** virus also came to be known as ***Marijuana,*** since both words are in the virus. Other researchers named ***Stoned*** for the geographical location in which they believed it had first been found. Hence it is also known as ***New Zealand, Australian, Hawaii, San Diego,*** and ***Smithsonian.*** Obviously not a unifying method for naming viruses, this has the further flaw that other completely unrelated viruses may be discovered in the same places. A further convention names viruses for the length they add to a file when they infect. =This is no use for boot sector viruses like ***Stoned,*** and leads to confusion with viruses whose length varies or which have the same length as each other. When there is a characteristic infective length, it can be useful for distinguishing variants of a single virus. Viruses have been named for the dates when their payload triggers, leading to a certain amount of competition for popular days, with several completely different viruses being known as ***Friday the 13th.*** The well-known ***Michelangelo*** virus is actually named for a date. There is nothing in the virus that refers to ***Michelangelo*** at all, but it triggers on March 6th, which is Michelangelo's birthday. Viruses can also be named for their payload, like ***Ping-Pong*** and ***Cascade,*** named for the screen effect they produce, and ***Yankee Doodle,*** named for a tune it plays. Unfortunately there are other viruses that borrow these effects, and sometimes are given confusingly similar names.

People who use more than one anti-virus product are often disturbed to find that they do not agree about the name of a virus. Sometimes they think that one product doesn't find the viruses that the other product finds, because it does not document them by the same names. The only way this confusion can be resolved is for everyone to realise that there is NO CORRECT NAME for any virus. We use the system we use for a number of reasons that make

sense to us. For one thing, it is the EICAR-approved convention as used by several anti-virus products. Other people use other systems that they prefer, each system tending to be used by a single product.

There is a naming standard, but it is mostly to do with what you cannot use as a name (someone's brand name, a company name, a living person's name, a geographical area 'where it was first found'). This standard is available from the University of Hamburg, together with a document giving the agreed Caro names for almost all existing viruses.

In this book, we list our preferred name first, and any other names we are aware of as aliases. Occasionally, we change our minds about a name (usually because an international naming agreement has been reached for that virus), or even rearrange part of the system of classification, so don't be too surprised if the names in this book do not always match the names reported by the on-line Virus Encyclopædia in Dr. Solomon's Anti-Virus Toolkit.

Additional information

Additional information about these viruses, and about viruses not covered in the printed documentation, is available in the on-line Virus Encyclopædia in Dr. Solomon's Anti-Virus Toolkit. There is also a book called 'PC Viruses'[2] available giving detailed information on about 100 of the most common viruses.

---

2 'PC Viruses: Detection, Analysis and Cure' by Dr. Alan Solomon *publ. Springer Verlag 1991*

Removal methods

Before doing a virus repair, we recommend that you switch off your PC and boot from a clean, write-protected DOS system diskette.

Method 1 Used for normal file, partition and boot sector viruses

1. Switch off the PC and boot from a clean DOS system diskette.
2. Run `FINDVIRU /REPAIR` to repair infected files, and partition and boot sectors. Alternatively, delete the infected files and replace them with clean copies.
3. Finally, check the disk again by running `FINDVIRU /DOALLFILES`.

   PLEASE NOTE: If you wish to scan inside archived files, refer to your Toolkit manual for details.

Method 2 Used for irreparable file viruses

1. Switch off the PC and boot from a clean DOS system diskette.
2. Delete infected files and replace them with clean copies. Alternatively, you can run `FINDVIRU /REPAIR /DELETE`.
3. Finally, check the disk again by running `FINDVIRU /DOALLFILES`.

   PLEASE NOTE: If you wish to scan inside archived files, refer to your Toolkit manual for details.

Method 3 Alternative method used for partition and boot sector viruses

For partition and boot sector viruses we recommend **Method 1** as shown above. However, the following alternatives can be used.

1. Switch off your PC and boot from a clean DOS system diskette and run **FINDVIRU** to identify infected diskettes and/or hard disks.
2. Run **CLEANBOO** to remove the virus from infected diskettes.
3. To remove a partition sector virus from the hard disk, run **CLEANPAR**. To remove a boot sector virus from the hard disk, either:

   Run `SYS C:` (from A:). **PLEASE NOTE:** SYS.COM must be from the same DOS version as is on the hard disk.

   or

   Run `CLEANPAR /H`.

The viruses

The Virus Encyclopædia is arranged like this:

Common Name

We use the name that has been standardised by EICAR, the European Institute for Computer Antivirus Research, and by CARO, the Computer Antivirus Research Organisation.

(Aliases)

Here we give some of the names used by other products to refer to this virus. Unfortunately, this list cannot be comprehensive.

Type	Boot sector, partition sector, file, other. **Boot sector** viruses infect the boot sectors of floppy disks, and either the boot sector or the partition sector of hard disks. **Partition sector** viruses infect the boot sectors of floppy disks, and the partition sector of hard disks. **File viruses** infect files. This may be just COM files, just EXE files, or both. Some viruses go memory resident. These are the ones that you are most likely to come across, as non-memory-resident viruses aren't sufficiently good at copying themselves to spread well. Multi-partite are both boot and file viruses **Companion** viruses create a COM file where previously there was only an EXE file. DOS runs the COM file in preference to an EXE file with the same name. **Overwriting** viruses overwrite the code at the start of the file with their own code – the original program then does not work. As a result, such viruses are so poor at spreading that you are highly unlikely to ever see one. See 1 About viruses for more detailed information.
Affects	Types of file affected.
File Growth	Amount by which files grow. Viruses add their code to the infected file. Boot and partition viruses, of course, do not, and neither do overwriting or companion viruses. The **File Growth** entry tells you by how much to expect to see a file growing. This value can be different for different files – some viruses round up the file size before infecting it; others deliberately have a variable size.
Removal	Removal method. Most viruses can be dealt with in one of three ways. Rather than repeat this information for each virus, refer to the methods described below.
Description	What it does and its effects.
Variants	What variants affect and their effects.

10 Past 3 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files between 4 and 64496 bytes are affected.
File Growth	748 bytes.
Removal	Method 1.
Description	On the 22nd of each month, the computer reboots. On various dates, various peripherals are disabled or made unreliable: 1st Keyboard 10th Hard disk 16th Monitor 29th Disks Between 15:10 and 15:13 each day, a keyboard trick is installed which causes the Ctrl or Shift key to be invoked, each with a 4.5% probability, on each keystroke.

Aids (Number 1)

Type	Overwriting file virus.
Affects	A COM file in the current subdirectory on execution of an infected file.
File Growth	Files are overwritten and grow to 13,952 bytes if they are smaller than that.
Removal	Method 2.
Description	The original program no longer works. With colour screens the system hangs. This virus has nothing to do with the Aids Information Diskette, a Trojan which was mailed to several thousand users in December 1989.

Aircop (None)

Type	Memory-resident boot sector virus.
Affects	Floppy disks.
File Growth	N/A
Removal	Method 3.
Description	The original boot sector is written to track 39, head 1, sector 9. The virus displays the message `RED STATE, Germ offensing --AIRCOP`.
Variants	There are a few variants: ***Aircot*** and ***AircopNG*** versions ***a***, ***b*** and ***c***.

Akuku (None)

Type	File virus.
Affects	COM and EXE files when an infected COM file is run. Files must be between 1,000 and 64,000 bytes long.
File Growth	COM: padded out to a multiple of 16 bytes, then 889 bytes added. EXE: padded out to a multiple of 16 bytes and 892 bytes added.
Removal	Method 1.
Description	At between 20 minutes and 23 minutes past each hour, if an infected program is run the message `A kuku, Nestepny komornik !!!` is displayed.
Variants	**Akuku-b:** As above, but displays the message `(C) by Metal Thunder IVRL MI`. **Copmpletely:** This says `Sorry, I'm copmpletly dead..` **Akuku-c:** One byte has been replaced with CCh, the one-byte interrupt. This was probably done accidentally by a virus researcher.

Alabama (None)

Type	Memory-resident file virus.
Affects	EXE files on execution.
File Growth	1,560 bytes.
Removal	Ensure the computer has been powered off, as this virus survives a warm boot, then use Method 2.
Description	Whenever a COM or EXE file is loaded, the next uninfected EXE file in the current subdirectory is infected. Read-only files are set to R/W, then reset after infection. When the hour changes, the message `SOFTWARE COPIES ARE PROHIBITED BY INTERNATIONAL LAW xxxxx 00000012 xxxxxxxxxxx Box 1055 Tuscambia ALABAMA USA` is triggered and the computer hangs. On a colour monitor the message is red and surrounded by a red blinking double-line box. Any file starting with DEBU or SYMD will not be infected but is modified to become unusable; this is aimed at DEBUG and SYMDEB. If the virus is in memory, the DOS **COPY** command and many other file-opening operations don't work properly. The virus will survive a warm boot (Ctrl Alt Del) and will continue to infect other programs afterwards.
Variants	There are two minor variants, ***a*** and ***b***.

Ambulance (Redx; Red Cross)

Type	File virus.
Affects	Two COM files in the current subdirectory or in the path, on execution of an infected file.
File Growth	796 bytes.
Removal	Method 1.
Description	When an infected file is executed, the virus looks for two COM files to infect, first in the current directory and then down the path. Every eighth (starting with the sixth) time an infected application is run, the ambulance is triggered. This is a small car which travels across the bottom of the screen with the two-tone siren of a German ambulance.
Variants	One variant triggers the ambulance every time an infected file is run; there is another minor variant.

Amoeba (1392; Khetapunk)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COM files smaller than 512 bytes and larger than 60Kb bytes are not affected. Date/time and read/write/hidden attributes are not preserved.
File Growth	1,392 to 1,407 bytes.
Removal	Method 2.
Description	The virus contains `KHETAPUNK - NOUVEL Band A.M.O.E.B.A. by PrimeSoft Inc` in encrypted form. The virus takes up 3Kb of memory when resident. There are no noticeable effects because of bugs in the code.

Angelina (Stoned.Angelina)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 1.
Description	This stealth boot and partition sector virus infects hard disks when booted from an infected floppy. Diskettes are infected on read and write access (e.g. the DIR command). Functionally, the virus is similar to *Stoned*. The virus contains the following encrypted text, which is never displayed: `Greetings for ANGELINA !!!/by Garfield/Zielona Gora`
Variants	There are two slightly different variants of the virus.

Anthrax (None)

Type	Partition and file virus.
Affects	COM and EXE files on execution of an infected file, and partition sectors.
File Growth	1,024 to 1,280 bytes.
Removal	Method 2, then Method 3.
Description	When an infected file is executed, another file is infected. The text `(c) Damage, Inc.` is in the file, indicating a Bulgarian origin, as is the word ANTHRAX. Some computers will not boot with ***Anthrax*** in the partition.

AntiCMOS (Lenart)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	This boot and partition sector virus infects the hard disk when booted from an infected floppy. Diskettes are infected on read or write access (e.g. DIR or COPY commands). The virus does not preserve the original boot and/or partition sector – it overwrites these with itself. On floppy disk access, the virus can trigger with a probability of approximately 1 in 256 times, and then patches CMOS data. Hard disk C: becomes 'not installed'. The drive type of floppy A: is changed as follows: If it was 5.25" 360Kb it becomes 3.5" 720Kb If it was 5.25" 1.2Mb it becomes 'not installed' If it was 3.5" 720Kb it becomes 5.25" 360Kb If it was 3.5" 1.44Mb it becomes 5.25" 1.2Mb If it was 'not installed' it becomes 5.25" 1.2Mb Since the virus does not bother to recalculate the CMOS checksum, the BIOS should display the CMOS CHECKSUM FAILURE error message on the next reboot.

AntiEXE (D3, NewBug, CMOS4)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy. Some EXE files
File Growth	N/A
Removal	Method 3.
Description	This boot and partition sector virus infects the hard disk when booted from an infected floppy. Diskettes are infected on read access (e.g. DIR command). When a certain (unknown as yet) EXE file is being executed or read from a disk (e.g. using the COPY command) the virus patches the first byte of the in-memory file image, thus causing unpredictable errors. In most cases the computer hangs.
Variants	There are two slightly different variants of the virus.

Anti-Pascal (AP-400; AP-440; AP-480; AP-529; AP-605)

Type	File virus.
Affects	A COM files between 2Kb and 64,000 bytes (but may vary: see below) on execution of an infected file.
File Growth	Bytes as indicated by the variant name.
Removal	Method 1.
Description	When an infected file is executed, the virus scans through the drives for another COM file to infect. **AP-400:** When there are no more files to infect, it deletes any files with the extension **?A?**. **AP-440:** When there are no more files to infect, it deletes any files with the extension **P??** or **BAK**. **AP-480:** When there are no more files to infect, it deletes any files with the extension **P??** or **BAK**. It also overwrites the directory entries by creating then deleting temporary files. **AP-529:** Affects files between 529 and 65,506 bytes. When it can't find any more files to infect, it deletes all BAK files and renames all PAS and EXE files to COM before deleting them. **AP-605:** Affects files between 605 and 64,930 bytes. When it can't find any more files to infect, it overwrites PAS files with itself and then renames them to COM files.

Anticad (Taiwan 3; Taiwan 4; Plastique; Invader; Hammer)

Type	Memory-resident file virus. Versions 1 and 4 (see below) are also boot sector viruses.
Affects	COM and EXE files on execution or copying.
File Growth	Anticad 1 4,096 to 4,111. Anticad 2 2,900 to 2,915. Anticad 3 3,004 to 3,019. Anticad 4 4,096 to 4,111. Anticad 5 2,576 to 3,103.
Removal	Method 1, then (for versions 1 and 4) Method 3. If the Trojan has triggered, run the system setup program, low-level format the disk, repartition and format it, then restore your backup.
Description	If a program called ACAD.EXE is run, the Trojan triggers. It disables the keyboard, clears the screen, overwrites drive A: (head 0 and all tracks), then does the same to drive B:. Next it overwrites drives C: and D: track 0, all heads, and works down the disk incrementing each track by an amount which itself increments for each step. Finally it overwrites CMOS with 0FFh and hangs the system. A less vicious variant is triggered 2,000 keystrokes after the last write, and disables hard disk writes. A third trick is to play music after a delay. There are three variants: Blue Danube Classical tune Chinese tune This virus looks as if it has been influenced by ***Jerusalem***.

cont...

	Anticad 5 does not contain the destructive routine, but plays music. This variant may predate ***Anticad 2*** which was previously thought to be the earliest. ***Anticad 5*** contains the following string: `To Whom see this: Shit! As you can see this document, you may know what this program is. But I must tell you: DO NOT TRY to WRITE ANY ANTI-PROGRAM to THIS VIRUS. This is a test-program, the real dangerous code will implement on November. I use MASM to generate various virus easily and you must use DEBUG against my virus hardly, that is foolish. Save your time until next month. OK? Your Sincerely, ABT Group., Oct 13th, 1989 at FCU.`

Arab (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Files must be more than 27 and less than 64,445 bytes long.
File Growth	834 bytes.
Removal	Method 1.
Description	The text `nsed Materi` can be found in the virus. After an infected file has been run 256 times, the virus patches the partition sector to make the hard disk non-bootable.

ARARA (None)

Type	File virus.
Affects	A COM file in the current subdirectory on execution of an infected file.
File Growth	Variable: 1,052 to 1,067 bytes.
Removal	Method 1.
Description	This non-resident virus is variable encrypted and polymorphic. Since the virus uses 80286-specific instructions, it will not operate properly on pre-80286 computers (most XTs). The virus has no payload. It contains the encrypted strings `[ARARA], *.OCM` and the following text: `ILASA MICALAZODA OLAPIRETA IALPEREJI BELIORE: DAS ODO BUSADIRE OIAD OUOARESA CAOSAGO: CASAREMEJI LAIADA ERANU BERINUTASA CAFAFAME DA IVEMEDA AQOSO ADOHO MOZ, OD MAOFASA. BOLAPE COMO BELIORETA PAMEBETA. ZODACARE OD ZODAMERANU! ODO CICALE QAA. ZODOREJE, LAPE ZODOREJE, LAPE ZODIREDO NOCO MADA, HOATHAHE SAITAN!`

Armagedon (The Greek)

Type	Memory-resident file virus
Affects	COM files on execution, except COMMAND.COM and files with ND as the sixth and seventh letters. Only files between 1,079 and 57,344 bytes are affected.
File Growth	1,079 bytes.
Removal	Method 1.
Description	The text `Armagedon the GREEK` is contained in the virus. Between 5am and 6am, the virus sends `+++aTh0m0s7=35dp081,,,,141` to the comms port. This has the effect of hanging up then dialling 081 141.

AT144 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Only works on machines with 286 processors and above.
File Growth	144 bytes.
Removal	Method 1.
Description	There is no payload.
Variants	There is a corrupted version which doesn't work. There are also 132-byte and 149-byte versions.

Attention (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files between 786 and 64,921 bytes are affected.
File Growth	394 bytes.
Removal	Method 1.
Description	The text string `ATTENTION!` will be found near the start of infected files. The critical error handler giving the DOS message **Abort, Retry, Ignore?** is permanently disabled.

Azusa (None)

Type	Memory-resident boot sector virus.
Affects	Floppy and hard disks.
File Growth	N/A
Removal	Method 3.
Description	There is no payload.

Backfont (V905; Topsy-905; Backfont-905)

Type	Memory-resident file virus.
Affects	EXE files on execution.
File Growth	900 to 905 bytes.
Removal	Method 1.
Description	Twenty seconds after infection, the screen fonts on EGA and VGA monitors are reversed. Some variants trash the hard disk.

Backtime (None)

Type	Memory-resident file virus.
Affects	COM files on execution, if less than 6,000 bytes long.
File Growth	528 bytes.
Removal	Method 1.
Description	The text string `Backtime` can be found in the virus, and the system clock appears to run backwards.
Variants	**Prague Blinker:** Files grow by 512 bytes. A blinker effect happens about once every 15 seconds. **Prague Joker:** Files grow by 496 bytes. On each timer tick (18.2 times per second) there is a 1 in 256 chance that the stack will be slightly corrupted. This leads to problems in running programs, and system crashes. **Prague Shaker:** Files grow by 152 bytes. The monitor seems to lose vertical synchronisation about once a second. This looks like a hardware problem.

Bad Boy (None)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	1,001 bytes.
Removal	Method 1.
Description	The virus is encrypted. It avoids being noticed by generic active monitors by using various techniques to get past traps for interrupt 13h.
Variants	**Bad Boy.a:** This contains the encrypted text `The bad boy halt your system...` and `The Bad Boy virus, Copyright(C) 1991.` **Bad Boy.b:** This contains the encrypted text `Make me better!` and `The Bad Boy virus, version 2.0, Copyright(C) 1991.`

Bad Guy (None)

Type	Overwriting file virus.
Affects	COM files in the current subdirectory when an infected program is run.
File Growth	None, but the first 264 bytes are overwritten.
Removal	Method 2.

Description	Because of the overwrite, infected programs no longer behave as they are meant to. There is a text string in the virus which says:
	
	`BadGuy virus (c) by Cracker Jack 1991 (IVRL)`
	`Italian Virus Research Laboratory (C) 1990, 1991`
	`IVRL Head Quarter, Milan Italy.`
	
	On Mondays, the virus reprograms the video controller for CGA monitors so that the horizontal trace is out of sync and the picture breaks up.

Bandit (None)

Type	File virus.
Affects	EXE files when an infected program is run.
File Growth	1,641 bytes.
Removal	Method 1.
Description	The string `!!PCBANDIT!!` can be found at the end of infected files. On Mondays the virus reformats the third floppy disk drive, device 2. This was probably meant to be the hard disk.

Bebe (None)

Type	File virus.
Affects	A COM file (unless set to read-only) on execution of an infected file.
File Growth	Padded to a multiple of 16 bytes, then 1,004 bytes are added.
Removal	Method 1.

Description	The text strings `VIRUS1`, `Skagi bebe` and `Fig Tebe!` can be found in the virus. If it can't find another file to infect, ten minutes after it's finished trying it pops a window up in the centre of the screen containing:
	
	`VIRUS!`
	`Skagi bebe`
	
	However, the virus hangs when it tries to install the interrupt to enable this.

Best Wishes (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COM files smaller than 512 and bigger than 60,000 bytes are not affected.
File Growth	1,024 bytes.
Removal	Method 1, then the DOS **SYS C:** command to repair the boot sector if the Trojan has triggered.
Description	At the end of the virus is the text string `This program ..With Best Wishes!`. Any infected program run on Friday 13th will first display the message `With Best Wishes!`. When you exit the program the message is displayed repeatedly. At the same time the boot sector is patched so that DOS thinks the disk has 0 sectors. On other days it reduces the count of the number of sectors by one cluster plus 256 sectors.
Variants	There are two, one of which grows files by 970 bytes and the other of which fails to infect EXE files. **BestWishes 1:** This does not use the INT2Fh tunnel to evade interrupt blockers, and the text message is `With Best Wishes`.

Better World (Fellowship)

Type	Memory-resident file virus.
Affects	EXE files on execution.
File Growth	1,019 to 1,034 bytes.
Removal	Method 2.
Description	The following text string can be found: `This message is dedicated to all fellow PC users on Earth Towards A Better Tomorrow And A Better Place To Live In` The string `03/03/90 KV KL MAL` may also be found (☞ ***Black Monday***). The file date and time are not preserved after infection. If the virus goes memory-resident during September, the message is displayed in 320x200 graphics mode each time a program is run. This is another derivative of ***Jerusalem***, and a close relative of ***Black Monday***.

Big Joke (None)

Type	File virus.
Affects	A COM file when an infected file is run. COMMAND.COM is not infected.
File Growth	1,068 bytes.
Removal	Method 1.

Description	If the system clock seconds counter stands at between 0 and 4 seconds when the virus is run, the following message is displayed:
	
	`At last.....ALIVE!!!!!`
	`I guess your computer is infected by the Big Joke Virus.`
	`Release 4/4-91`
	`Lucky you, this is the kind version.`
	`Be more careful while duplicating in the future.`
	`The Big Joke Virus, killer version, will strike harder.`
	`The Big Joke rules forever.`
	
	Each message is displayed in the centre of the screen, and is faded in and out by cycling through shades of blue.

Black Monday (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,055 bytes (EXE files may vary).
Removal	Method 1.
Description	The text string `Black Monday 2/3/90 KV KL MAL` can be found in the virus (☞ ***Better World***). When the virus is run on a Monday the Trojan is enabled. A counter counts down from 240 each time a file is infected, and when it reaches 0 a low-level format is done of head 1 on the hard disk, starting at cylinder 1 and stepping inwards. This virus appears to be a rewrite of ***Jerusalem***.

Blackjec (Bljec)

Type	File virus.
Affects	All write-enabled COM files in the current directory when an infected file is run. In most versions the date is set to the current date.
File Growth	Variable, depending on the version.
Removal	Method 1.
Description	There is no payload.
Variants	**Blackjec 3:** Files grow by 231 bytes. **Blackjec 4:** Files grow by 247 bytes; files which would increase the 64Kb COM file limit if infected are ignored. **Blackjec 5:** Files grow by 267 bytes, and files containing the string 'MZ' are not infected as they may be EXE files. **Blackjec 6:** As ***Blackjec 5***, but files grow by 276 bytes. Files conforming to CO*.COM are avoided. **Blackjec 7:** As ***Blackjec 6*** but files grow by 287 bytes and only three files are infected on each run. **Blackjec 8:** As ***Blackjec 7*** but files grow by 358 bytes and the date is preserved. **Blackjec 9:** As ***Blackjec 8*** but files grow by 369 bytes and the check for 'MZ' is different. There are also ***b*** versions of the variants listed above.

Blood (None)

Type	File virus.
Affects	A COM file of less than 32K on execution of an infected program.
File Growth	418 bytes.
Removal	Method 1.
Description	There is one chance in eight that the message `File infected by BLOOD VIRUS version 1.20` will be displayed. This is visible in the virus.

Boot droppers

These are not viruses themselves, but drop a virus when run, when they warn you that they are about to install a virus on drive A:.

S&S has seen droppers for ***Denzuk, Horse, Keydrop, Print Screen*** and ***Ogre*** to date.

Boys-500 (None)

Type	File virus.
Affects	COM files when an infected file is run.
File Growth	500 bytes.
Removal	Method 1.
Description	The virus contains the string `The good and the bad boy.` COM files are made read-only and EXE files have the system attribute set.

Brain (Pakistani; Pakistani Brain; Lahore; Ashar; UIUC)

Type	Memory-resident boot sector virus.
Affects	360Kb 5.25-inch floppy disks (even if not bootable). Hard disks are not infected.
File Growth	N/A
Removal	Method 3.
Description	The volume label of the infected floppy is changed to **(c) Brain** and infected disks have 3Kb of bad sectors. The following text can be found in the boot sectors in infected disks: `Welcome to the Dungeon (c) 1986 Brain & Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!` There are a number of major and minor variations in the actual wording, but the substance of the message remains the same. There is also a completely different message giving three telephone numbers. ***Brain*** replaces the boot sector of a diskette with its own code and moves the original boot sector further up the disk. Whilst the virus is in memory the boot sector looks normal, as the virus redirects any attempt to look at it and displays the original boot sector instead. The virus has no ill effects other than slowing down the floppy disk drive and making 7Kb of memory unavailable to DOS.
Variants	**Ashar:** An early version of Brain. There are six variants where the ***Brain*** message is different.

Brainy (Warrier)

Type	Memory-resident file virus.
Affects	COM files on execution. COMMAND.COM is avoided.
File Growth	1,527 bytes.
Removal	Method 1.
Description	The virus contains the text `The WARRIER!`.

Burger (None)

Type	Overwriting file virus.
Affects	A COM file on execution of an infected file. Some variants also infect EXE files.
File Growth	Most of the ***Burger*** variants are 560 bytes long, but this is unlikely to be noticed as the virus overwrites the start of the file.
Removal	Method 2.
Description	The virus overwrites the original program. The 792 version overwrites the first five sectors of drives C:, A:, D: and B: (in that order) if the system date is after February 1988. In one of the 560 versions, two random sectors of the first 256 are overwritten. In many other versions part of drive C: is overwritten. Most infected programs no longer function at all.
Variants	***382, 405.a, 405.b, 542.a – d, 560a*** to ***560.m, 1310.***

Burger-405 (None)

Type	Overwriting file virus.
Affects	COM files on execution of an infected file.
File Growth	Files smaller than 405 bytes grow to that size. Larger files don't change but no longer function.
Removal	Method 2.
Description	Infected programs no longer run.

Cara (None)

Type	Memory-resident file virus.
Affects	COM files on execution, opening, renaming or attribute change. Only files of more than 4Kb are affected
File Growth	1,025 bytes.
Removal	Method 1.

Description	The text `CARA` can be found near the start of the virus. The following strings can also be found:
	
	`Virus Es en memoria!`
	`Disco Es infectado. Reemplaza Boot.`
	`Clandestino Auto-Reproductivo Anti-virus`
	
	On every fourth access of a floppy disk, the virus checks the boot sector at offset 100h. If it finds one of six 2-byte signatures, it replaces the code of the boot sector with a non-infective one. ***Brain, Italian*** and ***Stoned*** are three viruses which this will clean. If it finds that memory is not a multiple of 16Kb, it displays `Virus Es en memoria!` followed by `Clandestino Auto-Reproductivo Anti-virus`.

Carioca (None)

Type	Memory-resident file virus.
Affects	COM files on execution (except COMMAND.COM).
File Growth	951 bytes.
Removal	Method 1.
Description	If the system year is 1989 or later, the month November or December, and the date the 15th or later, the Trojan is enabled. Every time a key is pressed the memory refresh timer is reprogrammed so the refresh takes longer and longer. Eventually the refresh takes so long the system hangs.

Cascade (Second Austrian; 1701; 1704; Blackjack; Autumn; Waterfall; Russian; Hailstorm)

Type	Memory-resident file virus.
Affects	COM files on execution, including COMMAND.COM.
File Growth	1,621 to 1,706 bytes, depending on the variant.
Removal	Method 1 or 2, depending on the variant.
Description	If the virus tries to infect a write-protected diskette the DOS **Abort, Retry, Ignore?** message is given. Cascade takes up 2Kb of memory when resident. If the system date is between October and December 1988, or the virus goes memory-resident when the year is 1980 and the year is subsequently set to 1989 or later, the virus produces a falling character display at random intervals. Characters detach themselves from their proper place on the screen and fall to the bottom of the display. As each character starts to fall the speaker clicks, so that the overall effect is rather like a hailstorm of characters. This virus uses one of the interrupts which Novell requires, and can cause serious problems on Novell networks. This is a very infectious virus. However, as the main variant has passed its trigger date it's difficult to detect without anti-virus software. The virus is encrypted to prevent casual disassembly and to fool automatic programs searching for virus characteristics.

cont...

Variants	There are several variants: **17Y4:** The third byte of the virus has been changed, which stops it from working properly. **1704-B:** Looks for IBB where the main version looks for IBM. The date tests have been changed to trigger it from August to December in all years except 1993. **1704-C:** As 1704-B, except for minor changes in the decryption and simply routines. **1704-Format:** This is another IBB version. The date tests have been changed to trigger it from October to December in all years except 1993. Instead of a screen display, a low-level format of heads 0 to 8 on track 0 is done, followed by a beep which continues indefinitely. **1621, 1661:** Two smaller variants. There are also a few minor variants of the ***1701*** version.

Casino (None)

Type	Memory-resident file virus.
Affects	COM files on execution. COMMAND.COM, files larger than 62,905 and those with the system attribute set are avoided.
File Growth	The file size is rounded up to the next multiple of 16 bytes and 2,330 bytes are added.
Removal	Method 1.
Description	When an infected program is run it infects the first COM file in the subdirectory and creates a hidden file called COMMAND(ff).COM where (ff) is the invisible character 0FFh. This file is used by the virus to go memory-resident, and then deleted. The increase in file size is masked if the virus is in memory. This is not always precise as the virus subtracts 2,330 bytes from the file size if the file is a multiple of 16 bytes (unless the file is smaller than 2,330 bytes), so some uninfected files appear smaller than they really are. On the 15th of January, April and August the Trojan triggers. The first 80 sectors of the current drive are read into memory; this includes the whole of the first copy of the FAT and normally part or all of the second copy. Garbage is written to the same 80 sectors. The following message is then displayed: `DISK DESTROYER A SOUVENIR OF MALTA I have just DESTROYED the FAT on your Disk!! However, I have a copy in RAM, and I'm giving you a last chance to restore your precious data WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER!! Your DATA depends on a game of JACKPOT CASINO DE MALTE JACKPOT`  `CREDITS : 5` `£££ = Your Disk` `??? = My Phone No.`  `ANY KEY TO PLAY`

cont...

	When you play, there are three possible results: 1. `HA HA !! You asshole, you've lost: say Bye to your Balls ...` and the machine hangs. 2. `No Fuckin' Chance; and I'm punishing you for trying to trace me down !` followed by the first message and a machine hang. 3. `BASTARD ! You're lucky this time - but for your own sake, now SWITCH OFF YOU COMPUTER AND DON'T TURN IT ON TILL TOMORROW !!!` and the FAT is copied back on to the disk.

Casper (None)

Type	File virus.
Affects	A COM file in the current subdirectory on execution of an infected file.
File Growth	1,200 bytes.
Removal	Method 2.
Description	If the virus tries to infect a write-protected floppy the DOS write-protect message is displayed. On April 1st the virus formats track zero of the floppy diskette in Drive A:. There is a message in the virus: `Hi! I'm Casper The Virus, And On April The 1st I'm Gonna Fuck Up Your Hard Disk REAL BAD! In Fact It Might Just Be Impossible To Recover! How's That Grab Ya! <GRIN>.` This message is part of the encrypted code, so it won't be visible in the virus. The virus was checked by setting the date to 1st April and running an infected program, and it did format track zero, head zero of the floppy drive; the hard disk was untouched. But because the registers were pointed to a non-legal track buffer, the diskette was unreadable.
Variants	This virus is derived entirely from ***Chameleon*** but the second layer of encryption is not present.

Catman (None)

Type	Boot sector virus.
Affects	Boot sector.
File Growth	N/A
Removal	Method 3.

Description	The virus includes the text string:
	
	`**********VIRUS PRODUCT`
	
	`BY WATCHIRA EM KMITNB V3.0 HIGH SPEED SEE YOU AGAIN IN NEW VIRSION`
	
	`DATA 9:1989 **********`
	
	The virus has only been seen in the form of a file, and if the file is run the machine hangs.

Chameleon (1260)

Type	File virus.
Affects	A COM file in the current subdirectory on execution of an infected file.
File Growth	Approximately 1,260 bytes.
Removal	Method 2.
Description	This is based on the book version of the 648 virus. It is written by the same author as ***V2P6*** – Mark Washburn of the USA. It appears to have been written to challenge anti-virus researchers, and has been encrypted on several levels so that it is very resistant to anti-virus techniques. It was the first polymorphic virus. The DOS critical error interrupt is not intercepted, so the usual message will appear if the virus tries to infect a file on a write-protected diskette.
Variants	***V2P2*** and ***Casper*** are very similar.

Chaos (Faust)

Type	Memory-resident file virus
Affects	COM and EXE files on execution.
File Growth	COM: 1,181 bytes; EXE: 1,184 to 1,199 bytes.
Removal	Method 1.
Description	On the 13th of each month, the virus sets up two conditions. First, it counts 50 keystrokes and then displays `CHAOS!!! Another Masterpiece by Faust!!!` and hangs the computer. Second, it sets up a Trojan on the disk interrupt, so that every fifth disk access causes a track to be overwritten. This is related to ***Jerusalem***.
Variants	There are four minor variants.

Chinese Fish (Fish Boot)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 1.

Description	This boot and partition sector virus infects the hard disk when booted from an infected floppy. It then infects floppy disk on read or write access (e.g. the DIR command).
	
	When active in memory, it stealths both the infected partition sector and the infected floppy boot sectors.
	
	If a disk infected with ***Chinese Fish*** is then infected with ***Stoned***, ***Chinese Fish*** removes ***Stoned***, leaving it infected with just itself.
	
	Starting in 1992, on the 1st, 11th, 21st and 31st of every month, when a PC is booted from an infected disk, the virus displays the following message:
	
	`Hello! I am FISH, please don't kill me.`
	`Congratulate 80th year of the Republic of`
	`China Building,Fish will help to kill stone`
	`Written by Fish in NTIT. TAIWAIN 80.10.18`

Choinka (Vienna-1881)

Type	File virus.
Affects	A COM file whenever an infected program is run. Only files between 10 and 60,000 bytes are affected.
File Growth	1,881 bytes.
Removal	Method 1.
Description	Between December 19th and 31st it displays its Christmas message – a large full-screen Christmas tree made of asterisks, and the message: `Merry Christmas & a Happy New Year for all my lovely friends from FATHER CHRISTMAS.` When a key is pressed the host program is run. This is yet another version of ***Vienna***.

Cinderella (None)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	390 bytes.
Removal	Method 1.
Description	The text `cInDeReL.1a` can be found in the virus. After 30,000 calls to interrupt 16h (the keyboard handler), not counting function 0 (read a character), a hidden file with the name CINDEREL.1A is created, containing 0 bytes.

Clipper (Jeru-Clipper)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,413 bytes. EXE files are first rounded up to a multiple of 16.
Removal	Method 1.
Description	The text `CLIPPER` can be found in the virus. On the 16th of each month, if an infected program is run the virus sets a flag when it goes memory-resident. The next time a program is run it triggers the Trojan, which overwrites the current drive starting with the boot sector and continuing on from there. This is based on ***Jerusalem***.

Com2Con (None)

Type	File virus.
Affects	The next uninfected COM file in the current directory when an infected program is run. Date and attributes are preserved, but infected files have the time set to 11:19.
File Growth	311 bytes.
Removal	Method 1.
Description	There is a 1 in 4 chance of COMMAND.COM being renamed to COMMAND.CON if it is in the current directory when an infected program is run. If this happens to the COMMAND.COM needed at start-up, the **Bad or missing Command Interpreter** message is displayed when the computer is next booted.

Crazy Daisy (None)

Type	Trojan. It relies on people copying it.
Affects	N/A
File Growth	N/A
Removal	Delete the Trojan and any patched files.

Description	When the program is run, an animated face in block graphics appears at the top left of the screen. When a key is pressed, the message:
	
	`Hi, I'm Crazy Daisy! I'll format your HARDDISK!`
	`Say Goodbye to Your files! Formatting...`
	
	The hard disk light flashes. The Trojan is creating a large hidden file of between 200 and 400Kb with a randomly chosen name, and containing **`Keep smiling! - Sun is shining!`** over and over again. It then displays **`ERROR: No SYSTEM found! No files on drive C: Insert SYSTEM diskette in drive A: and push any key!`**. If you do this, it looks at each EXE file on the diskette and patches it. When a patched program is run, it chooses one sentence at random, and each time a key is pressed displays another from its list. These sentences are:
	
	`Pretty day today - isn't it?`
	`Don't worry - sing a song!`
	`Life isn't easy!`
	`Don't hate Your computer! Let's be friends!`

Crazy Eddie (None)

Type	Memory-resident file and partition sector virus.
Affects	The partition sector when an infected file is run, and COM and EXE files on execution after starting up from an infected hard disk.
File Growth	2,600 to 2,700 bytes.
Removal	Method 2, then Method 3.
Description	The string `Crazy Eddie` can be found in the virus. On June 28th, or any Monday 28th, the virus trashes the hard disk by writing garbage to it.
Variants	There is a corrupted version which doesn't work.

Crew 1 (V2480)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	2,480 bytes.
Removal	Method 1.

Description	The text strings below are in the virus.
	
	After 1988, if the month is later than June, any infected program run results in a 3% chance that the following will be displayed:
	
	`This program is cracked by`
	
	`Notice this:`
	`TS ain't smart at all.`
	
	`Europcan`
	`Crackin'`
	`Crew`
	
	`Distribution since`
	`11-06-1987 (or 06-11-1987)`
	
	`Press any key`

Variants	***Crew 2***, with a length of 1,967.

D3 (AntiEXE)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks. Some EXE files.
File Growth	N/A
Removal	Method 3.
Description	This virus infects the hard disk when booted from an infected floppy. Floppy disks are infected on read access (e.g. DIR command). When a certain (as yet unknown) EXE file is being executed or read from a disk (e.g. COPY command) the virus patches the first byte of the file image in memory, causing unpredictable errors. In most cases the computer just hangs.
Variants	There are two slightly different variants.

Damage (Diamond-Damage)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,063 bytes. This is concealed if the virus is memory-resident.
Removal	Method 1.
Description	The text `DAMAGE!!!!` can be found near the end of the file. On Tuesdays, if an infected EXE file is run the virus low-level formats the third floppy drive (probably meant to be the hard disk). The other effect is a large multicoloured diamond in the centre of the screen, which shatters into smaller diamonds that bounce around the screen.
Variants	**Damage-b:** The strings `Jump for Joy!!!` and `DAMAGE-B!!` can be found near the end. The damage routine covers floppy drives A: and B: and well as the third floppy. Files grow by 1,110 bytes.

Danish Tiny (Kennedy)

Type	File virus.
Affects	All COM files in the current subdirectory on execution of an infected file. The DOS write-protect message is displayed if a write-protected floppy is accessed. Date/time and read/write attributes are preserved.
File Growth	333 bytes.
Removal	Method 1.
Description	When the date is June 6th, November 18th or November 24th, the message `Kennedy Er död - laenge leve The Dead Kennedys` is displayed, then the infected program is run. The dates are anniversaries of the deaths of members of the Kennedy family. One of a long series of ***Tiny*** viruses, with lengths of 163 to 1,000 bytes.

Dark Avenger 1800 (Eddie-1; Black Avenger; Diana)

Type	Memory-resident file virus.
Affects	COM and EXE files (see below). Only works on MS-DOS v3.0 and higher. Only files larger than 1,800 bytes are affected.
File Growth	1,800 bytes, subject to a rounding-up to the nearest 16 bytes.
Removal	Method 1, then run `SYS C:` using your version of DOS.

Description	A number of different actions on a file can trigger an infection:
	1. If copied, both the source and target are infected;
	2. If it is read;
	3. If the attributes are changed;
	4. If it is loaded and executed.
	Read-only files are made read-write, and the attribute reset after infection. The boot sector is used to store data.
	
	The virus writes a sector that starts `Eddie lives...somewhere in time!` at intervals to a random sector on the hard disk. This sector might not land on anything, or it might overwrite part of a program or some data. The damage is therefore subtle, and may escape detection for some time, eventually appearing on backups as well as on the hard disk.
	
	The virus includes two other messages which are not used:
	
	`This program was written in the city of Sofia (C) 1988-89 Dark Avenger`
	
	`Diana P.`

cont...

Variants	**Dark Avenger 2 (Eddie 2):** Files increase by 651 bytes. There is no payload, but the string `Eddie lives` can be found in the code. **Dark Avenger 2000 (Eddie 3; V2000; Die Young; Traveller):** Files larger than 1,958 are infected and grow by 2,000 bytes. When a program containing a copyright message from Vesselin Bontchev is run the system hangs. Vesselin is a Bulgarian anti-virus researcher. This was first found in Bulgaria, and contains the text `666`, as in the ***512*** virus. It uses many of the same ideas. The text `Copy me - I want to travel` is in the virus, but not displayed in one version. In another, it's `Only the good die young....` **Dark Avenger 2100 (Eddie-4; V2100):** Files grow by 2,100 bytes (concealed if the virus is in memory), and the virus contains the text `Eddie Lives`. It uses interrupt 13h to corrupt the disk by writing garbage to random sectors. There are two versions: in one, the SI register is used at various places, and in the other the DI register. It is a development from ***Dark Avenger 1*** and ***Dark Avenger 3***. **Ps!ko:** This is a simple hack of ***Dark Avenger 1800***. The messages have been replaced with `The Ps!ko Virus - Version 1.0, SiTT` and `The Ps!ko Virus - Written in the USA, (C)1991 by SiTT and The Violator`. Because of a mistake in reassembling the virus it can only replicate to one generation – second generation samples will not replicate. **MIR:** Infected files grow by 1,745 bytes. Near the start of the virus is the text `#.I.R. *-*-*-* Sign of the time!`. **1801:** A variant with a slightly different size. **1530, Milena, Slowdown** In the ***1800*** version there are also slight variants ***a, b, c, d, e, Rabid*** and ***Evil***.

Dark Avenger Slowdown (V1028; Slowdown)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. Only files larger than 1,028 bytes are affected.
File Growth	COM: 1,028 bytes; EXE 1,028 to 1,043 bytes.
Removal	Method 1.
Description	The computer is slowed down, and the slowing is proportional to the time of day. At midnight there is no slowing, at 1am there is one loop, at 2am there are two, and so on.

Dark Lord (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution or closing. COMMAND.COM is avoided. The date and time are not preserved.
File Growth	Rounds up to multiple of 16 bytes, then adds 921 bytes.
Removal	Method 1.
Description	The strings `Dark Lord, I summon thee!` and `MANOWAR` can be found in the virus. Interrupt ECh is defined as the old interrupt 21h.

Darth (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Avoids COMMAND.COM.
File Growth	None.
Removal	As the virus partly overwrites the file, it is best to use Method 2.
Description	The virus goes memory-resident by finding an area of zeroes in the segment from 9000h, copying itself there and patching the DOS function dispatcher to change the effect of function 40h(write to file). Thereafter, when a file is written to, the virus overwrites the first 253 bytes of that file. The files then no longer work. The string `Darth Vader` can be found in each version of the virus.
Variants	**Darth Vader-2:** This checks for 345 zeroes in the file. If it finds that many, it writes itself into the file. **Darth Vader-3:** This only needs 255 bytes of zeroes. **Darth Vader-4:** Needs 200 bytes of zeroes. Remove using Method 1.

Datacrime 1 (Columbus Day)

Type	File virus.
Affects	A COM file on execution of an infected file; files with D as the seventh letter (including COMMAND.COM) will not be infected.
File Growth	1,168 bytes.
Removal	**Datacrime 1, 1b:** Method 1. **Datacrime 2, 2b:** Method 2.
Description	When an infected file is run, the virus scans through the directory tree for an uninfected file; it also searches DOS devices in the order C:, D:, A:, B:. It recognises infected files by setting the last byte of the seconds field in the directory entry, which is not displayed by the **DIR** command. Every year from October 13th to December 31st, when it runs it displays the message `DATACRIME VIRUS RELEASE 1 MARCH 1989` and does a low-level format of the hard disk of cylinder 0 and all heads up to 8. If it tries to infect a write-protected disk, the DOS write-protect message is suppressed. The virus handles this incorrectly, and the next critical error encountered by DOS can crash the machine.
Variants	**Datacrime 1b:** Files grow by 1,280 bytes. **Datacrime 2, 2b:** Both COM and EXE files are infected. COM files grow by 1,480 bytes and EXE files by 1,500 to 2,000. When the virus triggers is displays `DATACRIME II VIRUS`.

Datalock (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on opening or execution.
File Growth	920 to 1,043 bytes.
Removal	Method 1.
Description	The virus contains the text `DataLock version 1.00`. When any file called *.?BF is opened on any date after August 1990 the machine hangs (although it was intended to do something else).
Variants	***a, b, c, d, e*** and ***f***. The ***f*** version is 1,043 bytes long; all the others are 920 bytes long.

David (Diamond-David)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COM files over 63,851 bytes are not infected.
File Growth	1,173 bytes. The increase is hidden.
Removal	Method 1.
Description	Because of a bug, infected COM programs don't work and are corrupted instead of being infected. The text `(C) David Grant Virus Research 1991 PCVRF` and `Distribuite this virus freely!!! ... ah ... John ... Fuck You!` can be found near the start of the virus. Because of the stealthing of file size, when **CHKDSK** is run with the virus memory-resident it will report inconsistencies between the sizes of infected files and the length of the FAT chain. If the computer is booted from a clean DOS disk and **CHKDSK** is run it will not report these false inconsistencies. On Tuesdays, the virus tries to format the hard disk but fails because of a bug.

Dbase (DBF)

Type	Part memory-resident file virus.
Affects	COM files on execution. Date/time and attributes are preserved.
File Growth	1,864 bytes. 1,884 bytes are subtracted from the top of conventional memory; this can be shown using **CHKDSK**.
Removal	Method 1.
Description	The **Abort, Retry, Ignore?** message isn't disabled, so write-protected diskettes give the correct message. DBF files are garbled by interchanging pairs of bytes. The virus also creates a hidden file in the root directory called **C:\BUGS.DAT** which contains the list of garbled files. Three months after the file is created, a damage routine should trigger. The same thing happens if the system date is set to three months before the date of **BUGS.DAT**. Because of a bug in the code, the damage routine doesn't work. If it did, it would write garbage over the first 256 sectors on the hard disk, overwriting the boot sector, both copies of the FAT, and the whole directory. It would do this to every device attached to the computer, starting at drive D: and working up to drive Z:. On a system with no drive D: the system would hang, and on networks the network software won't permit a direct write to the drive.

Deicide (None)

Type	Overwriting file virus.
Affects	A COM file in the root directory of drive C: (except COMMAND.COM) on execution of an infected program.
File Growth	None. The first 666 bytes of the file are overwritten.
Removal	Method 2.
Description	The text `DEICIDE! Glenn(666) says : BYE BYE HARDDISK!! Next time be carufull with illegal stuff.....` can be found near the beginning of the virus. After each infection, the message `File coruption error` is displayed. If the virus can't find an uninfected file to infect in the root of drive C: it overwrites the first 80 sectors of the drive.
Variants	***Deicide-2*** is a non-overwriting virus, infecting COM files and adding 1,335 bytes to them. Use Method 1 to remove it.

Demon (None)

Type	Overwriting file virus.
Affects	All COM files in the current subdirectory on execution of an infected file.
File Growth	None. The first 271 bytes are overwritten.
Removal	Method 2.
Description	Because of the overwrite, infected programs no longer do what they used to do. A text string in the virus says `Demonhyak Viri X.X (c) by Cracker Jack 1991 (IVRL).` On Tuesdays, the virus overwrites the first 160 sectors of drives A: to J: and then displays `Error eating drive C:`.

Den Zuk 2 (Venezuelan; Search)

Type	Memory-resident boot sector virus.
Affects	Floppy disks. Hard disks are not infected.
File Growth	N/A
Removal	Method 3.
Description	Once the virus is in memory, its infection counter (initialised to 8) is decremented every time a diskette is accessed. When the counter reaches 0 the infection process is triggered and the counter reset to 2. On systems with a colour monitor, when Ctrl Alt Del is pressed the text `Den Zuk` is displayed in red with a symbol to the side of the screen which looks like a stylised globe. The volume label of an infected diskette is changed to Y.C.I.E.R.P. There are two text messages in the virus which are not displayed. At the beginning is `Welcome to the Club -The HackerS- Hackin' All The Time` and at the end is `The HackerS`. ***Den Zuk*** replaces the boot sector of a diskette with a 360Kb boot sector of its own. This gives problems with floppies of a higher capacity. The virus also uses track 40, head 0, sectors 33 to 41 to store code and the bit-map of the logo. This has no ill-effects on 360Kb floppies but will overwrite data on track 40 of any higher-capacity diskette. If the virus finds ***Brain*** or ***Den Zuk 1*** on the boot sector, it overwrites them with itself. If Ctrl Alt Del is pressed, a reboot is triggered and the logo is displayed. ***Den Zuk*** marks the diskette as ***Brain***-infected, so that ***Brain*** will not infect it.

cont...

Variants	**Den Zuk 1 (Ohio):** An early version. When a warm boot is performed a box is displayed containing the message `(c) 1988, The HACKERS Technology Bandung 40254 - Indonesia`. **Den Zuk 3:** When an infected machine is rebooted a blue box is displayed in the centre of the screen containing the message `(c) 1988, The HACKERS Technology Bandung 40254 - Indonesia`.

Destructor (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, opening, renaming, attribute setting or date/time access. COM files between 50 and 64,000 bytes are infected.
File Growth	COM: 1,150 bytes. EXE: padded to nearest multiple of 16, then another 1,150 added.
Removal	Method 1.
Description	There are two text strings in the virus: `DESTRUCTOR V4.00 (c) by ATA` and `The Time is my !`. There is no payload.

Devil's Dance (941; Mexican)

Type	Memory-resident file virus.
Affects	COM files on execution. Date/time are not preserved.
File Growth	941 bytes each time they are infected. When they exceed the 64Kb limit they will not run.
Removal	Method 1, then if necessary run **CleanPart** which *may* be able to lay down a working version of the partition sector.

Description	Every time the infected machine is rebooted the message:
	
	`Have you ever danced with the devil under the weak light of the moon?`
	`Pray for your disk!`
	`The__Joker ...`
	`Ha Ha Ha Ha Ha Ha Ha Ha Ha Ha`
	
	is displayed.
	
	If you reboot after the virus has gone memory-resident and a few thousand keystrokes have been entered, the virus overwrites the partition sector with garbage after displaying this message. Next time the computer is started it will appear not to have a hard disk. In addition, after a few keystrokes each character is displayed in a different colour.

Variants	**Devil's Dance.b:** The partition sector is not overwritten.

Dewdz (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	601 bytes.
Removal	Method 1.
Description	The text `Kewl Dewdz!` and `Made in STL (c) '91` can be found encrypted in the virus. Each time an infected program is run, there is a 21% chance that the virus will move the cursor to row 12 column 35, display `Kewl Dewdz!` and restore the cursor position.

Diamond (V1024)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. Date/time and read/write attributes are not changed.
File Growth	1,024 bytes. If the virus is in memory the growth is hidden from **DIR** commands.
Removal	Method 1.
Description	If the computer has a colour monitor being used in text mode, the virus display triggers on the hour. This starts as a multi-coloured diamond made up of four smaller diamonds in the centre of the screen. After a brief pause the smaller diamonds scatter and bounce around the screen independently. Every time they pass over a character they blank it so the screen is gradually cleared except for the bouncing diamonds.
Variants	**Diamond-b:** As above.

DIR II (None)

Type	Memory-resident file virus.
Affects	COM and EXE files whenever their directory entry is accessed. As a result, this virus spreads very quickly.
File Growth	None apparent, but an extra cluster is loaded when the file is executed.
Removal	Method 2. Replace the infected executables from clean copies. Alternatively, it may be easier to back up data files, reformat the disk, and reload the data.
Description	When the virus goes memory-resident it copies its code to the last cluster on the disk. It infects by patching the directory entries. There is no payload apart from the crosslinking.
Variants	There are a few minor variants of this virus.

Dirvir (Dir)

Type	Memory-resident file virus.
Affects	An uninfected COM file when a **DIR** is requested.
File Growth	691 to 760 bytes. Growth is concealed if the virus is in memory.
Removal	Method 1.
Description	When an infected file is run there is a 1 in 256 chance that the first two sectors of the FAT will be overwritten with garbage.

Discom (Jeru-Discom)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. Files with names starting with ACAD are not infected.
File Growth	COM: 2,053 bytes. EXE: padded to nearest 16 bytes, then a further 2,053.
Removal	Method 1.
Description	There is a counter in the last byte of the file.. When this reaches 80 the Trojan is triggered, which writes one sector of rubbish to the hard disk each time an infection takes place. This virus is based on ***Jerusalem***.

Disk Filler (Filler-6)

Type	Memory-resident boot and partition sector virus.
Affects	Floppy and hard disks.
File Growth	N/A
Removal	Method 3.

Description	When the computer is booted from an infected floppy the virus infects the partition sector of the hard disk. When the computer is booted fro the hard disk the virus goes memory-resident and infects each floppy disk accessed in any drive. On hard disks, the virus goes to sectors 0 to 7, and on floppies to the track after the last track on the disk.
	
	The following text appears in the virus:
	
	`Haha, varus van a gepben!! Ez egy eddig meg nem kozismert varus. De hamarosan az lesz. A neve egyszeren toltogeto. Ezt a nevet onnan kapta, hogy feltoltogeti a FAT-tablat kolonbozo alakzatokkal. Ez nar meg is tortent!!!`
	
	The virus uses stealth to hide the infected boot sector.
	
	If 26 minutes pass without disk access, the Trojan triggers. It overwrites the FAT with a picture that looks like this:
	
	`oooooo oooooo`
	`o o oo o`
	`o o o oo o o o`
	`o oo o`
	`o oooo oo oooo o`
	`o o o o`
	`oooo oooo`
	
	The character used is ASCII 1 (the smiling face). The message above is then displayed.

DoomII.1240 (Taiwan DoomII.1240)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,240 to 1,255 bytes.
Removal	Method 3.
Description	The virus contains the encrypted text `DOOM II (c) Dr.Jones, NCU`. Four sectors of drive C: are overwritten. In March, there is one chance in six that the first track of the hard disk will be overwritten each time an infected application is run. At the same time, the first track of each floppy disk currently in a drive is overwritten.

DoomII.752 (Taiwan DoomII.752)

Type	Memory-resident file virus.
Affects	A COM file on execution of infected files.
File Growth	752 bytes.
Removal	Method 2.
Description	On the 8th of each month, the current hard disk is trashed, as are the first 320 sectors of drive D:. It then displays `DOOM I, (c) NCU Taiwan`.

Doteater (None)

Type	Memory-resident file virus
Affects	A COM file smaller than 63,488 bytes when an infected program is run.
File Growth	944 bytes.
Removal	Method 1.
Description	When COMMAND.COM is infected and the computer is booted, a face enters from the right-hand side of the screen and eats every dot you type, complete with sound effects. Pressing [^] cancels the effect.

DSME.Teacher (DSME:Demo)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COM files longer than 50,152 bytes are not affected.
File Growth	Variable: 3,240 to 3,590 bytes.
Removal	Method 1.

Description	The virus is variably encrypted and highly polymorphic.
	
	There is no payload. The virus contains the encrypted strings:
	
	`Teacher virus ( A demo virus for DSME to all teacher )`
	
	and
	
	`DSME v1.0`

Dyslexia (Solano)

Type	Memory-resident file virus
Affects	A COM file on execution. Date/time and read/write/hidden attributes are preserved. COMMAND.COM is avoided. Critical error handling is disabled, so attempts to infect a file on a write-protected floppy disk are not reported as errors by DOS.
File Growth	2,000 bytes.
Removal	Method 1.
Description	12.25 minutes after the virus goes TSR it picks a random position on the screen. If there is a figure there and in the position to the right it swaps them. It repeats this every 73 seconds. This works on colour and mono screens in text mode.
Variants	**Dyslexia dropper:** This drops ***Dyslexia*** into memory. The dropper is not itself a virus, but once it is in memory every COM file run will be infected.

EDV (None)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks.
File Growth	N/A
Removal	Method 3. Unfortunately, by putting the original boot sector at (39,0,8), ***EDV*** partly overwrites a file or subdirectory.
Description	When the computer is booted from an infected (not necessarily a boot) diskette the virus goes memory-resident. While it is, any write-enabled floppy disk accessed is liable to be infected. Hard disks become non-bootable, although accessible. Memory is not reduced, so memory map programs and monitors may not see this virus becoming resident. The message `MSDOS Vers. E.D.V.` can be found on infected boot and partition sectors. The virus replaces the boot sector of a diskette with its own code and moves the original boot sector further up the disk. In the case of a hard disk, it moves the partition sector and replaces the original with its own code. While the virus is in memory it counts the number of diskettes it infects, and after the sixth the damage routine is triggered. The count is reset if the computer is rebooted before the sixth infection. The damage routine writes garbage over the first and second hard disk, then over the first four floppy drives. This means all drives on most computers. The garbage is written on to cylinders 0 and 1, heads 0 to 3; this will overwrite the partition record, the boot sector, both copies of the FAT, and the directory, on most disks. It then displays `That rings a bell, no? From Cursy.` If the virus is in memory, it tries to hide itself. If you try to read the boot sector the virus displays the original sector, not its own version.

Eight Tunes (1971)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COM files between 8,177 and 63,310 bytes are affected. EXE file greater than 8,177 are also infected. Read/write and date/time are preserved.
File Growth	1,971 bytes.
Removal	Method 1.
Description	When a file is first infected, the virus stores the current date as the number of days since January 1st 1984. When an infected file is run and the system date is 91 days or more after that, it chooses a tune from a repertoire of eight and plays it about 30 minutes afterwards. The tune most likely to be recognised is Auld Lang Syne; the others are Nobody Knows the Trouble I've Seen, four German rambling songs, a series of random notes, and the interrupt 8 handler re-interpreted as music. After it's played the first tune, it waits for a few minutes and repeats the choice of a random tune, then continues to play the tune every few minutes. The virus does its own memory management, so may not be detected by monitors or memory map programs.

Empire (Evil Empire)

Type	Boot and partition sector virus.
Affects	Hard and floppy disks.
File Growth	N/A
Removal	Method 3.
Description	When the computer is booted from an infected diskette (not necessarily a bootable one) the virus copies itself to the hard disk. While the virus is present it infects any disks or diskettes accessed. There are a large number of variants, as the author of the virus kept changing it to evade the anti-virus detection system used by the University of Alberta.
Variants	***1, 2, Botany, a, b, c, d, #2, Canadian, Non-Canadian, U of A, UA, B.4, B1, Evil, D1, D2.***

Empire.Monkey.A (Monkey)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks.
File Growth	N/A
Removal	Contact S&S Technical Support for help (see below).
Description	The stealth virus has no payload, and contains the encrypted string `Monkey`. The virus encrypts original uninfected boot or partition sectors and does not preserve partition table information. This causes no problems while the virus is active in memory – due to the stealth techniques used, a normal partition sector is returned. But when booted from a clean floppy an infected hard disk is inaccessible, so tha virus cannot be removed using Method 3.
Variants	***Empire.Monkey.B*** contains some pieces of code rearranged, but is otherwise almost identical.

Enigma (None)

Type	File virus.
Affects	A COM or EXE file on execution of an infected file.
File Growth	1,755 bytes.
Removal	Method 1. You will need to replace corrupted files.
Description	Near the end of the virus is the text `This is the voice of the Enigma virus.....the spirits of the hell are coming back! (C) 1991 by Cracker Jack * Italy *.` On Sunday or Monday it formats track 20, head 0 of the floppy disk in drive A: and attempts to reboot the computer. Some machines just hang. This virus is a plagiarised version of ***Old Yankee***.
Variants	**Enigma.b:** The effects are triggered on Saturdays.

Espejo (15 years)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 1.

Description	When the virus is memory-resident, it infects hard disks and diskettes being read (e.g. with the DIR command).
	
	On the 7th April, or any other date if the virus infected ten disks since the last boot, the virus triggers and switches to its destructive mode. Any disk being accessed after this is overwritten with the following text (in Spanish):
	
	`Esto te pasa por programas que a nosotros nos cuesta tanto trabajo hacer. Que te quede de Experiencia, Mexico,1994`
	
	The virus also intercepts interrupt 16h (BIOS Keyboard Services). It then occasionally simulates typos by adding 5 to the character code being entered from the keyboard. For instace, A changes to F, B to G etc.
	
	The virus contains the text string:
	
	`This Virus is from MEXICO, I have 15 years old`

Etc (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	700 bytes.
Removal	Method 1.
Description	The text `Virus, (c) ETC` and `E.T.C.VIRUS, Version 3.0, Copyright (c) 1989 by E.T.C. Co.` can be found in the virus. The first time the infected program is run, the message `Virus, (c) ETC` is displayed before the program runs.

Evil (Live after Death 3; Phoenix Evil)

Type	Memory-resident file virus.
Affects	COM files on opening, except those over 64Kb and some others. This means about 1 file in 8 is ignored. Some EXE files are also Trojanised.
File Growth	1,701 bytes. COMMAND.COM is infected without increase.
Removal	Method 2, then check how much FAT corruption has been caused. Some data files will be corrupted; examine each file and restore the backup if necessary.
Description	The text `The evil that men do lives on and on...` is encrypted in the virus. The encryption and the decryptor/loader are both variable, so there is no consistent search string. The FAT is gradually corrupted by the occasional swapping of two entries while they are in the sector buffer; this means that anything monitoring disk writes fails to see the corruption, as it happens in memory and DOS does the write. In addition, at interrupt 13h level some disk reads are converted to writes.
Variants	This is part of a long series from Bulgaria.

Exebug.a (Exe_Bug)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks. Some EXE files.
File Growth	N/A
Removal	Contact S&S Technical Support for help (see below).
Description	This stealth virus can survive a clean boot. When a PC is booted from an infected diskette, the virus infects the hard disk and patches the CMOS to disable the A: drive. Thus, when you try to boot from a floppy,, the infected partition sector is loaded instead. The virus gains control, stays memory-resident and simulates a normal boot from the A: drive. When the virus is memory-resident, it infects hard and floppy disks being read (e.g. DIR command) and demonstrates stealth techniques, concealing the changes made to boot and partition sectors. When an EXE file is being written to disk (e.g. LINK or COPY commands), under certain circumstances the virus can trojanize the file. EXE files being written to A: can be trojanized to become the ***Exebug*** virus dropper. On execution, such a program deletes all the files in the current subdirectory, infects the hard disk, then terminates. EXE files written to drives other than A: can be turned into instant trojans, trashing all data on the hard disk when executed. Since the virus patches CMOS to disable drive A: to bypass the clean boot, you cannot use Method 3 to remove it. Even if you set up CMOS to re-enable drive A: and boot from a clean system floppy, the hard disk will be inaccessible since the virus overwrites the partition table information in the infected partition sector.
Variants	There are four other ***Exebug*** variants known. Some of them do not disable drive A: and thus cannot survive a clean boot.

Exterminator (None)

Type	Overwriting file virus.
Affects	All COM files in the current subdirectory on execution of an infected file.
File Growth	None. Overwrites the first 451 bytes.
Removal	Method 2.
Description	Infected programs no longer work as they should. There is text in the virus which says: `Exterminator 1.0 - (c) by Cracker Jack 1991 (IVRL) Italian Virus Research Laboratory (C) 1990,1991 Message to Virus Researchers: Non rompetemi le palle o mi arrabbio... Non so Se sono stato abbastanza charo... Exterminator Virus 1.0 (c) by Cracker Jack 1991 (IVRL) No panic...this is a Harmless Virus...`  On Mondays, the virus overwrites the first 160 sectors of drive C:. It then displays `Exterminator Virus 1.0 (c) by Cracker Jack 1991 (IVRL) No panic...this is a Harmless Virus...`

F-You (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	417 to 635 bytes.
Removal	Method 1.
Description	The text **`Fuck you!`** can be found in the virus. 55 minutes after the virus goes memory-resident the screen clears and the message appears in the middle. It stays there for a while, then disappears and you can continue. This is repeated every hour.

F1-337 (None)

Type	Memory-resident file virus.
Affects	COM files on execution or opening. COMMAND.COM is avoided.
File Growth	337 bytes.
Removal	Method 1.
Description	There is no payload.

Faggot (None)

Type	File virus.
Affects	COM files on execution of an infected file.
File Growth	1,009 bytes.
Removal	Method 1.
Description	The virus contains the string `Hi Guy! Nice to meet you! I an the little FAGGOT virus!` and some obscene messages. The virus always trashes drive C: by overwriting it with 800 sectors of garbage, after the displaying the message above. On March 7th it's meant to format drive C:, but this doesn't work. The virus trashes the hard disk before trying to infect a file, so it never actually infects a file.

Falling Letters Boot (None)

Type	Memory-resident boot sector virus.
Affects	Floppy and hard disks, when booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	The boot sector is moved further up the disk and replaced with the virus's own code. On floppy disks the boot sector is moved to (39,1,6). The virus triggers a falling letters display.

Fichv (None)

Type	File virus.
Affects	All COM files in the current subdirectory more than 1,500 bytes long when an infected file is executed.
File Growth	896 to 903 bytes.
Removal	Method 1.
Description	The text `FICHV 2.1 vous a Eu` can be found in the virus. During March it will trash the disk by writing the above message to the first six sectors of each track. The virus is encrypted and attempts to resist disassembly by using interrupts 1 and 3.
Variants	Version 1.0 infects EXE files, adding 897 bytes; version 2.0 infects COM files, adding 896 bytes.

Filedate 11 (USSR)

Type	File virus.
Affects	An EXE file on execution of an infected file. All infected files are given the date and time August 17 1988, 2:08am.
File Growth	571 to 586 bytes.
Removal	Method 2. If the Trojan is triggered, **CleanPart** *might* be able to repair the damage.
Description	Each time an infected program is run there is a 3% chance that it will overwrite the partition sector of the hard disk.

Filehider (V789)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files smaller than 63,488 bytes are affected.
File Growth	789 bytes.
Removal	Method 1.
Description	Every Friday there is a 1 in 16 chance of the Trojan triggering; on Friday 13th this becomes a 1 in 4 chance. The Trojan makes all files in the current subdirectory hidden.

Fish (Fish6)

Type	Memory-resident file stealth virus.
Affects	COM and EXE files when any disk access involving them is made. COMMAND.COM is infected first.
File Growth	3,584 bytes. The size is concealed. This is a fully stealthed virus.
Removal	Method 1.
Description	The virus code is concealed from scanners, and hides for much of the time. This makes the computer run so slowly that the presence of the virus becomes apparent to the naked eye. At any time during 1991 or later, the virus announces itself with the message `FISH VIRUS #6 - EACH DIFF - BONN 2/90 '~knzyvo}'` and hangs the computer. Any computer with the date set correctly will therefore find it spontaneously. There are a number of side effects, including slow running, wasted disk space because of growing files, and sometimes data file corruption because the virus gets confused and infects a non-executable file. The `~knzyvo}` string becomes **TADPOLES** if you subtract 42 from the code for each character.
Variants	The message implies that at least 5 other variants exist, but none have been seen or reported. However, each file infection is encrypted with a different key, so each appears different.
	Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS diskette, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will *NOT* be seen by DOS. For this reason, it is strongly recommended that the Anti-Virus Toolkit be used from the original write-protected floppy disks until the virus has been eradicated. FindVirus will find *Fish* in memory, even after it has taken control of the computer.

Flash (Blink)

Type	Memory-resident file virus.
Affects	COM files between 1,000 and 64,303 bytes, and EXE files, on execution.
File Growth	688 bytes.
Removal	Method 1.
Description	At any time after June 1990, seven minutes after the virus goes memory-resident it blinks the screen display four times and repeats this every seven minutes. If you single-step through the virus code it reboots instead of running. This happens because when the virus patches the code just a few bytes past the execution pointer, that patch is ignored because the CPU chip has already read the code in.

Flip (Omicron)

Type	Memory-resident file and partition sector virus.
Affects	COM and EXE files on execution. COM files must be smaller than 62,857 bytes.
File Growth	2,343 bytes. EXE files vary slightly. If COMMAND.COM has been infected the increases are hidden.
Removal	Method 1, then Method 3.
Description	The virus contains the encrypted text `OMICRON by PsychoBlast`. The encryption and the encryptor/loader are variable. At 10am on the second day of the month, if the computer has been booted from an infected partition, there is a monitor reversal on EGA and VGA screens. The date is obtained from CMOS memory so this only works on AT and PS/2 machines.
Variants	***2343.a, 2343.b, 2153***

Form (None)

Type	Memory-resident boot sector virus.
Affects	Hard and floppy disks. When the computer is booted from an infected (not necessarily boot) floppy, the virus goes memory-resident and infects any disk accessed thereafter.
File Growth	N/A
Removal	Method 3.
Description	On the 18th of each month, each key beeps when you press it, and infected diskettes have 1Kb in bad sectors. There is a message in the virus which never gets displayed: `FORM doesn't destroy data! Don't panic! Fuckings go to Corinne.` ***Form*** is a very common virus.

Frodo (Century; 4K; 4096; IDF; Hidden)

Type	Memory-resident file virus.
Affects	A COM or EXE file on almost any operation.
File Growth	4,096 bytes. This increase and the bytes of which it consists are hidden when the virus is memory-resident. This virus is fully stealthed.
Removal	Method 1. Depending on the damage, **CleanPart** *might* be able to lay down a new partition sector.
Description	Self-recognition is provided by adding 100 years to the file date; this will not be noticed as DOS only displays the last two digits of the year. If the virus is in memory, any program looking at the date is given the original one. The virus is intended to install a small routine on the partition sector of hard disk and the boot sector of floppies in drive A:. When the computer is booted from such a disk it was intended to display large letters made out of block characters saying `FRODO LIVES!` surrounded by a neon-like display around the edge of the screen. This was meant to happen every day from September 22nd to December 31st. The hard disk becomes inaccessible. In all known instances, this routine is corrupted and the machine simply hangs. However, there are at least two versions, of which one is less corrupt than the other.
	Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS diskette, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will *NOT* be seen by DOS. For this reason, it is strongly recommended that the Anti-Virus Toolkit be used from the original write-protected floppy disks until the virus has been eradicated. FindVirus will find *Frodo* in memory, even after it has taken control of the computer.
Variants	**Frodo-b:** Replicates as above, but if it did the partition drop (which still doesn't work) the partition record dropped would not work as several bytes have been nulled out.

Frogs (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	1,500 bytes.
Removal	Method 1.
Description	On the 5th of each month, when an infected program is run the virus displays the message `(V) AIDS R.2A - Welcome to Frog's Alley!, (c) STPII Laboratory - Jan 1990` after exiting. It also deletes the first file in the current subdirectory.

Fu Manchu (2086)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except COMMAND.COM.
File Growth	2,086 bytes. EXE files grow by 2,080 to 2,095 bytes.
Removal	Method 1.
Description	When a warm boot is performed, the message `The world will hear from me again!` is displayed. If the date is after August 1st 1989, the virus monitors the keyboard buffer. If 'Fu Manchu' is typed, the virus types back `Fu Manchu virus 3/10/88 - latest in the new fun line!`. If the name 'Thatcher', 'Reagan', 'Waldheim' or 'Botha' are typed, it adds in 'xxxx' which is one of four obscenities.. If either of the two most common English four-letter swear words are typed, it backspaces over them. The computer will also be rebooted at random intervals. The virus creates a TSR to do perform these effects, taking 2Kb of memory. This virus appears to be a rewrite of ***Jerusalem***.

Fumble (Typo; Typo Com)

Type	File virus.
Affects	All COM files in the subdirectory on execution of an infected COM file. Files are not re-infected. Infection only takes place on even dates. Date/time and read/write attributes are preserved.
File Growth	712 to 867 bytes.
Removal	Method 1.

Description	The **Abort, Retry, Ignore?** message isn't disabled, so appears when an attempt is made to infect a write-protected diskette.
	
	The virus occasionally replaces the letter typed with that of the key immediately to the right using the following table:
	
	`'1234567890-=\~!@#$%^&*()_+`
	`|qwertyuiop[]asdfghjkl;'zxcvbnm,./`
	`QWERTYUIOP{}ASDFGHJKL:";`
	`ZXCVBNM?`
	
	The fumble only activates if you type faster than 60wpm. If you type at that speed, you get a fumble if the keyboard is untouched for 5 seconds. There is code in the virus which should gradually decrease the gap but it doesn't work correctly.

Variants	**Fumble.b:** Files grow by 755 bytes. ***Fumble.c*** and ***d*** are minor variants.

Gergana (None)

Type	File virus.
Affects	A COM file in the current directory on execution of an infected file.
File Growth	182 bytes.
Removal	Method 1.
Description	The text `Gergana` can be found in the virus.

Ghostballs (Ghost)

Type	File virus.
Affects	The next uninfected COM file in the same subdirectory on execution of an infected file. Attributes are preserved. The critical error handler is not disabled, so any attempt to infect a write-protected floppy will still display the usual message.
File Growth	2,351 bytes.
Removal	Method 1. It isn't necessary to remove the non-infective ***Italian*** code from the diskettes, but if you wish you can use **CleanBoot**.

Description	The code contains the message:
	
	`Ghostballs, Product of Iceland`
	
	`Copyright (c) 1989, 4418 and 5F19`
	
	which is never displayed.
	
	When an infected application is run, the virus tries to read the boot sector of the diskette in drive A:. If this attempt is successful, it drops a copy of ***Big Italian*** (with all infective code removed) on to the boot sector.

GP1 (Jeru-GP1)

Type	Memory-resident file virus.
Affects	Executable files on execution, but only when IPX (part of the Novell shell) is loaded. Only files between 4 and 64,496 bytes are affected.
File Growth	COM: 1,813 to 1,845 bytes; EXE: 1,526 to 1,573 bytes.
Removal	Method 1.
Description	The text `GP1 Removed from memory` can be found in the virus. This is intended to be a demonstration of how to steal login passwords using IPX calls. Because of a number of bugs it doesn't work. This virus is closely related to ***Jerusalem***.
Variants	There is also a version where the password stealing routine works.

Greemlin (Diamond-Greemlin)

Type	Memory-resident file virus.
Affects	COM (from 1,146 to 63,878 bytes) and EXE (over 1,164 bytes) files on execution.
File Growth	1,146 bytes. This is concealed if the virus is in memory.
Removal	Method 1.
Description	The text `greemlin` can be found in the virus. If an infected EXE file is run on June 14th, the virus trashes the first six sectors of the first three floppy disks. If it is a Tuesday it trashes the first six sectors of track 4, head 0 of drive A:. A screen display can be triggered at any time.

Green Caterpillar (1575)

Type	Memory-resident file virus.
Affects	COM and EXE files when a directory is examined. The next uninfected executable file in that directory is infected. This virus only works on an AT or PS/2 with a CMOS clock.
File Growth	COM: 1,583 to 1,591 bytes. EXE: as COM, but may vary slightly.
Removal	Method 1.
Description	At any time after two months from the date of infection, provided the screen isn't mono MDA, the caterpillar is triggered. The caterpillar has a green body, a yellow head and a red mouth; it starts at the top left of the screen and works its way across, line by line from top to bottom. It eats characters and drops them out of its rear end, displaced by 10 characters to the left and converted to yellow on black.
Variants	*a, b, c.*

Grower-268 (V270X)

Type	File virus.
Affects	The next uninfected COM file on execution of an infected file.
File Growth	Each generation is one byte bigger than the last, so the growth is 268 bytes or more.
Removal	Method 1.
Description	The virus is encrypted.

Guppy (None)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	152 bytes.
Removal	Method 1.
Description	There is no payload.

Hallöchen (Hello 1a)

Type	Memory-resident file virus.
Affects	Uninfected COM and EXE files on execution, unless: dated the current month; COM files less than 5,000 and more than 63,510 bytes. There is also a test for EXE files (more than 5,000 bytes and less than 64Kb), but they all pass. Read/write and date/time are preserved.
File Growth	2,012 to 2,027 bytes.
Removal	Method 1.
Description	This virus was found in Germany, so the messages are in German: `Hallöchen !!!!!!, Here I'm` and `Acrivate Level 1.` these are not displayed. After 50 infections the machine gradually slows down. If the number of infections is greater than 70, it adds a keyboard handler in which 70 is subtracted from the infection count and the result divided by 2. This then becomes the number of chances out of 256 for any given keystroke to be corrupted. The corruption consists of 1 being added to the ASCII value for all values over 32, so A becomes B, B becomes C and so on.

Hate (Klaeren)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except COMMAND.COM and COM files larger than 63,852 bytes.
File Growth	978 to 1,000 bytes.
Removal	Method 2.
Description	The virus is encrypted. In May 1991 the virus trashes the CMOS and displays the message `Klaeren Haß, Haß!.` There is some relationship with ***Jerusalem***.

Headcrash (None)

Type	Memory-resident file virus.
Affects	The next COM file in the directory on execution of a program. Files must be between 1,792 and 61,696 bytes, and the current day must be an odd-numbered day.
File Growth	1,067 bytes.
Removal	Method 1.
Description	On odd-numbered days, if a program is loaded in a five-minute window in each hour, the message `Headcrash Industries celebrate 0054 hex` is displayed, where 0054 is replaced by a counter of the number of programs run. The five-minute window is variable depending on the instance of the virus.

Hero (Siskin-Hero-506)

Type	Memory-resident file virus.
Affects	COM files on execution. Files can be re-infected.
File Growth	506 bytes.
Removal	Method 1.
Description	The virus uses the upper half of the interrupt vector table for storage. On the first day of the month a message is displayed. This is encrypted in the file and the decryption doesn't appear to work as the message displayed is blank.

Horse (Hacker; Naughty Hacker)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution and reading.
File Growth	1,154 bytes. The increase is hidden from the **DIR** command.
Removal	Method 1.
Description	The text `Sofia,Jan 1991 (c) Naughty Hacker` can be found in the virus. When a counter reaches 0, a sound is made on the speaker and the screen displayed is interfered with, changing the horizontal synchronisation to a new value. The counter is initialised to 13,398 and decremented each time DOS is called.
Variants	**Horse 2 (Hacker 2):** Files grow by 1,160 (version 2b) or 1,158 (version 2). They are infected when they are run, closed or read, and the date in the text string is 'Feb '91'. All effects are the same except there is no sound. **Horse 3 (Hacker 3):** Files grow by 1,594 (version 3.1) or 1,610 (version 3). They are infected when they are opened, created, read, run, or when various other DOS functions are called. COMMAND.COM is avoided. The growth is hidden from **DIR** and other programs checking the sizes. The strings `Naughty Hacker` or `N. Hacker` (version 3.1) can be found in the virus. Single-step tunnelling is used to get under interrupts 13h, 21h and 2Fh. There are no other effects. **Horse 4 (Hacker 4):** Same as ***Horse 3***, except that files grow by 1,776 bytes. Each time a DOS function call is made, a counter (initialised to 9,029) is decremented. At zero, a routine is installed on the timer tick which interferes with colour screens.

cont...

	Horse 5 (Hacker 5): As ***Horse 3*** , but files grow by 1,576 bytes. **Horse 6 (Hacker 7):** As ***Horse 3*** except that files grow by 1,594 bytes. Disk reads are occasionally converted to writes and vice versa, when a file is closed. **Horse 7 (Hacker 7):** As ***Horse 1***, except that the date in the text is changed to `Jan.Feb 1991`.

Horse Boot (None)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks when the computer is booted from an infected floppy (not necessarily bootable) disk.
File Growth	N/A
Removal	Method 3.
Description	**Hard disks:** The original partition table is moved from (0,0,1) to (0,0,7), and the virus installs itself in its place. **Floppy disks:** The original boot sector is moved to (39,1,9) and the virus installs itself in its place.

Hungarian-482 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files between 254 and 64,000 bytes are infected.
File Growth	482 bytes.
Removal	Method 1.
Description	On November 7th, if an infected program is run the message `Format ...` is displayed, and the virus writes rubbish progressively down the hard disk starting with the partition. It only overwrites head 0 and the first cylinder because of a bug.

Hybryd (None)

Type	File virus.
Affects	COM files on execution of an infected file.
File Growth	1,306 bytes.
Removal	Method 2. If the boot sector has been Trojanised, boot from a clean DOS disk and run `SYS C:`.
Description	The string `AKUKU` can be found in the code. On and after Friday 13th 1992 the virus drops a Trojan on to the boot sector of the current drive and trashes 1 file in 8 by patching the first 5 bytes. There is a 1 in 4 chance it will set the number of floppy drives to 1 and the memory to 256Kb in the equipment byte. The Trojan first displays the message: `Wirus v. 1.0 (c) Hybryd Soft Specjalne podziekowania dla Andrzeja Kadlofa i Mariusza Deca za artykuly w Komtuterze 11/88` then it formats cylinder 10, head 0 of the drive and displays **`Formatowanie zakonczone.`** This is a development of ***Vienna***.

Hymn (None)

Type	Memory-resident file virus.
Affects	COM and EXE files larger than 2,816 bytes on execution, opening, creation, closing, renaming or attribute change.
File Growth	1,865 to 1,977 bytes.
Removal	Method 1.
Description	The strings `.WV.` and `ussr` are found in the virus. When the date equals the month (January 1st, February 2nd etc.) the virus alters the boot sector, replacing the OEM label with IBM 3.3, and Russian music is played.
Variants	**Sverdlov:** Files grow by 1,962 bytes. The virus goes TSR without using any DOS calls and the text string `.VS.` can be found in the virus. **Hymn-2144:** This is a larger version. When this triggers, it also nulls the BPB data on the boot sector. With some versions of DOS this means that the computer cannot be booted even from a floppy disk. If this occurs, try booting from a different version of DOS. Use Method 3 to repair the boot sector.

Icelandic (Saratoga; Disk eater; Disk crunching)

Type	Memory-resident file virus.
Affects	EXE files on execution a counter means that every alternate file is infected). Date/time are not preserved; the resident part of the virus takes 2Kb of memory.
File Growth	632 to 647 bytes – it also depends on the version.
Removal	Method 1.
Description	The virus goes TSR without using any DOS calls so some detection software may not find it. Every time a file is infected, the virus tries to mark a bad sector on the hard disk. Because of the way it does this, the attempt will fail until a certain number of files are infected. After that, the number of bad clusters will increase with the number of infected files. ***Icelandic*** does its own memory management, so memory mappers and monitors may not detect it.
Variants	**Icelandic 1-b:** Every tenth program is infected. **Icelandic 2:** This doesn't use interrupt 21h for file reading and writing, but searches for the relevant code and makes a far call to the routine there. This is to defeat any anti-virus software which detects illegal writes to EXE or COM files by assuming that all file reads and writes go via interrupt 21h. This version doesn't mark bad clusters on the hard disk, but infects every tenth program. **December 24th:** A development of ***Icelandic 2***. EXE files grow by between 848 and 863 bytes, and every tenth file is infected. If the virus goes memory-resident on December 24th the message `Gleîleg jòI` is displayed instead of the program being run. A big difference between this and the older ***Icelandic*** viruses is that the date/time is preserved and the DOS critical error handler is disabled to avoid the **Abort, retry, Ignore?** message. However, there is a bug in the code here and if there is a critical error the machine is likely to hang.

Incom (None)

Type	File virus.
Affects	All COM files in the current subdirectory on execution of an infected file.
File Growth	648 bytes.
Removal	Method 1.
Description	The virus is encrypted. There is a 10% chance that the palette displayed on an EGA or VGA monitor will be changed.

Int13 (None)

Type	Memory-resident file virus.
Affects	Uninfected COM files on a directory request. It will only infect files larger than 512 bytes and with at least 512 bytes of slack space between the end of the file and the end of the cluster. Only files between 4 and 64,496 bytes are affected.
File Growth	None.
Removal	Method 2.
Description	The text `Int 13` can be found in the virus. The virus takes effect only with a colour monitor; if the system has a mono monitor the system will hang.

Internal (1381)

Type	File virus.
Affects	EXE files (chosen randomly) on execution of an infected file. The files infected depend on the contents of the header.
File Growth	1,381 to 1,467 bytes.
Removal	Method 1.

Description	If an infected file is run 90 days or more after the infection, the Trojan is triggered. This consists of a letterfall followed by the message:
	
	`INTERNAL ERROR 02CH`
	`PLEASE CONTACT YOUR HARDWARE MANUFACTURER IMMEDIATELY!`
	`DO NOT FORGET TO REPORT THE ERROR CODE!`
	
	The infected file is then disinfected.

Variants	2C as above; there is also a version where the 2C in the message is replaced by 2E.

Itavir (None)

Type	File virus.
Affects	The next uninfected EXE file in the current subdirectory on execution of an infected program.
File Growth	1,600 to 7,000 bytes.
Removal	Method 2.

Description	This virus reads and writes the files without using interrupt 21h, by using interrupts 25h and 26h and decoding the FAT. This will evade many memory-resident virus detectors.
	
	If the number of the month is even, the date is the 21st and the time is 3pm or after, the Trojan is triggered. The keyboard is disabled and the following message is displayed:
	
	`.......AHI..AHI..AHI........`
	`Ho proprio l'impressione di essere un Virus`
	`Maligno......`
	`Molto maligno (maturalmente)`
	`Non vi rimane che da azionare l'interruttore`
	`AUGUR!!!........`
	
	Then all sectors of all logical drives are overwritten with garbage.

IVL (HIV-1)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution or opening. COM files must be between 1,614 and 64,000 bytes and EXE files between 1,614 bytes and 64Kb.
File Growth	1,614 bytes.
Removal	Method 1.
Description	The string `HIV Virus - Release 1.0 Created by Cracker Jack (C) 1991 Italian Virus Laboratory` can be found in the virus. Every Saturday the above message is displayed each time and EXE program is run, instead of running the program. Between 4pm and 5pm the screen trick is triggered, which consists of a face character which bounces around the screen rather like ***Ping Pong***. This is in the same family as ***Swami***.

Jabberwocky (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. EXE files are infected by conversion to the COM structure, so only files of 65,024 bytes or less are infected.
File Growth	812 bytes.
Removal	Method 1.
Description	The text `JW2` **can be found near the start of the file.** Occasionally, when an infected program is run, it beeps and the message `BEWARE THE JABBERWOCK` appears.
Variants	A previous version which only infected COM files was not released by the author, according to the author. This one is 615 bytes long.

Japanese Christmas (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	600 to 653 bytes.
Removal	Method 1.
Description	Every December 25th, the virus displays in the centre of the screen the message `A merry christmas to you` cycling through the colours (green, yellow, blue, magenta, light blue, white etc.) and blinking the characters as it goes.

Jeff (June 7)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	Padded to a multiple of 16 bytes, then another 812 bytes.
Removal	Method 1.
Description	On the 7th of each month after June 1991, after infecting the next file the virus displays `Jeff is visiting your harddisk...` it then overwrites 126 sectors of drive C:, starting with the first sector of the FAT, and hangs the computer.

Jerusalem (1813; Hebrew University; Israeli; Friday 13th; Frère; Russian; Black Friday; Jerusalem-B; JV; Morbus Waiblingen; Black Hole; sUMsDOS; Payday)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except COMMAND.COM.
File Growth	COM: 1,813 bytes. EXE: 1,808 to 1,823 bytes. COM files are not re-infected. EXE files grow each time they are infected until they are too large to load into memory. Some EXE files are infected without growing, usually because the genuine EXE is followed by overlays in the same file. The virus uses 2Kb of memory as a TSR. Occasionally an EXE is not infected correctly and fails to run as soon as it's infected.
Removal	Method 1. Note that there is a bug in ***Jerusalem*** which causes it to mis-infect some EXE files (such as Windows programs) and overwrite part of their code. These files will have to be replaced; **FindVirus** will notify you of them.
Description	Every Friday 13th, when a program is run it is deleted. On any date, 30 minutes after the virus has installed itself a PC XT system slows down to a fifth of normal speed; on faster machines the slowdown is not as noticeable. At the same time, if the system is in text mode, a small black rectangle opens up, as the portion of the screen from row 5 column 5 to row 16 column 16 is scrolled up by two lines. ***Jerusalem*** uses functions of interrupt 21h that Novell requires, and so is incompatible with Novell. Possible symptoms of this include workstations becoming disconnected from the network and the generation of large spool files. ***Jerusalem*** disables critical error handling so that any attempt to infect a write-protected diskette does not result in the usual DOS error messages.

cont...

Variants	***Jerusalem*** is the most common file virus, and because of this the code has been modified by a number of virus authors. The following are closely based on ***Jerusalem***:
	
	The Suriv viruses:
	These are early, less sophisticated predecessors of ***Jerusalem***. Suriv 1 and 2 trigger on April 1st and Suriv 3 on Friday 13th. These viruses are not removable.
	
	Sunday (Jeru-Sunday):
	Files grow by about 1,636 bytes, and every Sunday at approximately half-hour intervals the following text is supposed to be displayed:
	
	`Today is SunDay! Why do you work so hard?`
	`All work and no play make you a dull boy!`
	`Come on ! Let's go out and have some fun!`
	
	It is also supposed to delete every program as it is executed. However, there is a bug in the virus and none of this works.
	
	Sunday.b:
	This is a working version of ***Sunday***.
	
	Sunday 1.b:
	As for ***Sunday***, but a bug in the critical error handler which caused a problem on write-protected disks has been corrected.
	
	Sunday 1.d:
	As for ***Sunday***, but a bug in the critical error handler which caused a problem on write-protected disks has been corrected in a different way.
	
	Sunday 1 Tenseconds:
	As for ***Sunday***, but the delay is 10 seconds and the test for Sunday has been corrected to day 0 (instead of day 7).
	
	Sunday 2:
	As for ***Sunday***, but files grow by 1,733 bytes.

cont...

	Anarkia: Almost identical to ***Jerusalem***, but uses the self-recognition code Arkia. **PSQR:** Files grow by about 1,720 bytes, and on the 13th of each month any program run is deleted. In addition, junk is written to the hard disk partition sector and the nine sectors after it. The self-recognition code is PSQR. **Jerspain (Jeru-Spanish):** On the 26th of each month, any program run is deleted. **Frère:** The virus plays Frère Jacques on Fridays and the 13th of each month. **Jerusalem-Westwood (Westwood):** Files grow by about 1,829 bytes, and on Friday 13th each file run is deleted. **Jerusalem-113b:** Programs will not run on any Saturday. COMMAND.COM is infected, and instead PHENOME.COM is avoided. **Jerusalem-Apocalypse:** The text `Apocalypse!!!` can be found in the virus, and the self-recognition code is C.J**. Every Friday 17th each file run is deleted. **Jerusalem-Czech:** On Friday 13th the virus deletes each program run. Both the self-recognition and code placement are different from the original. **Jerusalem-T1:** On Tuesday 1st, all files run are deleted.

cont...

Jerusalem-T13:
COM and EXE files grow by 1,812 bytes. It deletes programs executed on Tuesday 13th.

Jerusalem-Sat13:
Deletes programs executed on Saturday 13th.

Jerusalem-Frère.2:
Once a minute the virus plays Frère Jacques. There is also a variant called ***Two Tigers*** which plays the same tune.

Jerusalem-Nemesis:
Same as ***Jerusalem,*** including Friday 13th deletion, but avoids infecting NEMESIS.COM instead of COMMAND.COM. It contains the string `NEMESIS.COM`.

Jerusalem-Captain Trip:
Contains the strings `Captain Trips` and `SPITFIRE`. If the year is not 1990 and it is a Friday on or after the 15th, every time a program is run an empty file is created with the same name. On other dates it installs a routine in the timer tick which triggers after 15 minutes. On June 16th it reprograms the video controller. The virus doesn't work properly.

Jerusalem-J:
COM files grow by 1,237 bytes and EXE files by 1,232 (after rounding to a multiple of 16). All ***Jerusalem*** effects have been removed.

Jerusalem-Yellow:
Files grow by 1,363 bytes. After 45 minutes, or after 4,096 keystrokes, a big yellow square with a shadow pops up in the centre of the screen and the computer hangs. This version does not repeatedly infect EXE files.

Friday-15th (Skism):
Files grow by 1,813 bytes. On Friday 15th, the virus creates a file with the same name whenever a program is run.

Jerusalem-Jan25:
Every January 25th every program run is deleted.

cont...

	Carfield (Jeru-Carfield): Files grow by 1,508 bytes, and on Mondays every 42 seconds the string `Carfield!` is displayed. **Mendoza (Jerusalem Mendoza):** If the year is 1980 or 1989 it does nothing. Otherwise, when the virus goes TSR, if the floppy disk drive motor count is 25 a flag is set. This will happen if the program is run from a floppy disk drive. If the flag is set, every program run is deleted. In years other than 1980 and 1989, if the delete flag is not set, 30 minutes after the virus is installed the cursor is changed from its current state to a block. After an hour, it switches Ins, Caps Lock, NumLock and Scroll Lock to Off. Minor variants: ***Standard.SuMsdos, Standard.AA33CCDDEE, Standard.null, Standard.UMsDos, Standard.Var, Standard.Nocommand, Jan25, a, Anarkia.2, Puerto, Spanish, Messina, ffd, 1af, Critical, Flag_ee, *a204*, Frère2, Frère3, 2e7, Not13, b0f, Phenomen, 52f, 7c01, 6d46, JVT1, J, Friday15, 3503, Feb-7th,*** Nov30, ***sUMFDos, SKISM, 5a4, 65d6, BSA, Turkish, Dragon.*** The name ***Friday 13th*** is applied to this virus, but also to two unrelated viruses: ***Friday 13th*** and ***Virus-B***.

Jojo (None)

Type	Memory-resident file virus.
Affects	COM files on execution, including COMMAND.COM. It does not disable the **Abort, Retry, Ignore?** message when accessing a write-protected diskette. Takes 2Kb of memory when resident.
File Growth	1,701 bytes.
Removal	Method 1.
Description	The text `Welcome to the JOJO virus` is near the beginning of the virus, and near the end is `Fuck the system (c) - 1990 xxxxxxxxxxxxx zzz.` If an infected file is run after 7pm it triggers a kaleidoscope display if run on a colour screen. Mono systems simply hang. This is a version of ***Cascade*** (the 1701 version), extensively hacked. The letterfall code has been replaced by the kaleidoscope effect, and the encryption and decryption routines are not called.
Variants	**Dazzler:** This is a harmless program which gives a dazzling screen effect. Jojo's author used it as a subroutine in Jojo; some scanners search for that code, giving a false alarm.

Joker (Jocker; Wabik)

Type	Overwriting file virus.
Affects	EXE files on execution of an infected file.
File Growth	None. Files are overwritten.
Removal	Method 2.
Description	The virus copies itself to another file, overwriting it. Programs no longer work. The infected file must be called WABIK.EXE or it will not infect others.

Joker-01 (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. Only infects COM files smaller than 6,795 and EXE files smaller than 6,656 bytes.
File Growth	29,233 bytes, most of which is a bitmap of the display.
Removal	Method 1.
Description	The last eight bytes of infected files form the message `JOKER-01..` When the virus triggers, a full-screen animated picture of the Joker is displayed in colour.

Joshi (Joshua)

Type	Memory-resident boot and partition sector virus.
Affects	Floppy and hard disks when booted from a floppy (not necessarily a bootable) diskette. Any write-enabled diskette accessed can be infected.
File Growth	N/A
Removal	Power off the computer, as ***Joshi*** survives a warm boot, then use Method 3.
Description	**Floppy disks:** This replaces the boot sector of a diskette with its own code and moves the original boot sector further up the disk. The boot sector of floppies is moved to a safe place, except on 720Kb diskettes where a bug in the virus causes it to write the body of the virus on to track 40. **Hard disks:** It moves the partition sector and replaces it with its own code. This causes problems on a few hard disks where the displaced partition overwrites part of the FAT. Every January 5th it saves the current screen to memory and replaces it with a display in 40-column mode in large type on a blue background with a double-line border, which says `Type 'Happy Birthday Joshi'!`. This remains in place until the user types as requested, then the original screen is restored.

July 13 (None)

Type	File virus.
Affects	An EXE file on execution of an infected file. Files with an EXE extension but no MZ signature (on the first two bytes) are deleted.
File Growth	1,201 bytes.
Removal	Method 2.
Description	On July 13th it installs a screen changer on to the timer tick.

Jumper (French Boot, SillyBop)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 1.
Description	This boot and partition sector virus infects the hard disk when booted from an infected floppy. Unlike most viruses of this kind, ***Jumper*** does not intercept interrupt 13h (BIOS Disk Services). Instead, it intercepts interrupt 1Ch (User Timer Interrupt) and waits until DOS is loaded. Then it intercepts interrupt 21h (DOS Services), as do many file viruses. Whenever DOS Change Disk or Buffered Input services are called (e.g. when a user types A: or B: at the DOS prompt), the virus attempts to infect a diskette in drive A:. When booted from an infected disk, the virus triggers with a probability of 1 in 32. It falls into an infinite loop, filling the screen with ASCII character 238 (0EEh).
Variants	There are two slightly different variants of the virus.

June 16th (Pretoria)

Type	File virus.
Affects	All uninfected COM files on the current disk (or any COM file on the drive referred to in the command) on execution of an infected file. Date/time are preserved, but attributes aren't. The DOS write-protect message is displayed if a diskette is write-protected.
File Growth	879 bytes, or to a minimum size of 1,758 bytes.
Removal	Method 1.
Description	This virus is very visible as it scans the whole directory tree looking for uninfected files to infect. Every June 16th it scans through the root directory of the current drive, reading one sector at a time and converting any filename it finds to **ZAPPED**, with the attribute of a normal file; thus subdirectories are no longer subdirectories.

June 4 (Bloody)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks on booting from a floppy (not necessarily bootable) disk. Subsequent floppies are infected from the hard disk.
File Growth	N/A
Removal	Method 3.
Description	After 128 hard disk boots, and thereafter every 6, it displays `Bloody! Jun.4, 1989`. **360Kb diskettes:** The boot sector is copied to (0,1,3). This is the seventh directory sector, which is rarely used. **1.2Mb diskettes:** The boot sector is copied to (0,1,3). This is the third directory sector, and if it's in use a directory listing which starts OK ends up as gibberish. **Hard disks:** On a tiny percentage (such as those set up originally using DOS 2.0) the place where the partition sector is copied to (0,0,6) is the fourth FAT sector, which will trash any files using it. This is based on ***Stoned***, but is very different.

Junkie (None)

Type	Memory-resident multipartite virus.
Affects	COM files, partition sector of hard disks, boot sectors of floppy disks. this virus does not infect the boot sector of 360Kb floppies.
File Growth	Variable between 1,027 and 1,041 bytes.
Removal	Method 1.
Description	This virus was the subject of much media hype when it was first dicovered in Ann Arbor, Michigan – in truth there is little special about it. During infection, the virus disables the TSRs in the Microsoft and Central Point Anti-Virus products. The virus only becomes memory-resident on booting, not from executing an infected COM file. It is, however, a fast-infector, meaning that if the virus is not detected in memory it can be easily transferred to a COM file.

Justice (None)

Type	Memory-resident file virus.
Affects	DOS 3.1 and 3.30 only. COM files on execution, opening, renaming or attribute change. Files larger than 64,272 bytes are not affected, neither are IBMBIO.COM, IBMDOS.COM or COMMAND.COM.
File Growth	1,242 bytes.
Removal	Method 1.
Description	The text `...AND JUSTICE FOR ALL` can be found in the virus. Every time there is a disk write, a counter is incremented. If the write is to cylinder 0 (FAT or directory, depending on the geometry of the disk), the counter is reset to 0. If the counter reaches 246 the write is redirected to the cylinder one less than the target cylinder.

Kamasya (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,098 bytes.
Removal	Method 1.
Description	The text `Kamasya nendriya prtir labho jiveta yavata jivasya tattva jijnasa nartho yas ceha karmabhih` can be found in the virus. Every Tuesday the above message is displayed. This virus is related to ***Swami***.

Kampana-3445 (None)

Type	Memory-resident file virus, and partition sector virus dropper.
Affects	Program files on execution. A copy of ***Telefonica*** is dropped into the partition sector, and replicates in the usual way. It doesn't do this if ***Stoned*** is present.
File Growth	3,445 bytes but highly stealthed, and doesn't show for any of the five DOS calls giving the size.
Removal	Method 2, then Method 3.
Description	The message in the virus says `(C) 1990 Grupa HOLOKAUSTO (Barcelona, Spain) KampanaAnti-TELEFONICA: Mejor servicio, enores tarifas...` and is encrypted, as is the entire ***Telefonica*** code dropped in. There is a relationship between this and both ***Fish6*** and ***Frodo***.

Kemerovo (V257)

Type	File virus.
Affects	All COM files in the current subdirectory on execution of an infected file.
File Growth	257 bytes.
Removal	Method 1.
Description	Each time an infected file is run there is a 10% chance that the computer will reboot.

Keydrop (None)

Type	Memory-resident boot sector virus.
Affects	Hard and floppy disks on booting from an infected floppy (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	The text `(c) Copyright 1990 Keydrop inc.` can be found in the virus, and it uses 5Kb of memory.

Keypress (Twins; St Leos; 9.8min)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. If DOS 2 is running, files are also infected when they are read.
File Growth	1,232 to 1,487 bytes.
Removal	Method 1.
Description	Every 10 minutes, for a period of two seconds the virus adds five more of the same key to any keypress.
Variants	***a, b, c, d, e, Samsoft.*** ***Samsoft*** puts a message on the screen.

Keytrick (None)

Type	Trojan.
Affects	N/A
File Growth	N/A
Removal	Method 3.
Description	Every 256th keystroke has a 1 in 4 chance of being ignored.

Kiev-483 (None)

Type	File virus.
Affects	A COM file in the current subdirectory on execution of an infected file. Only files between 50 and 61,440 bytes are infected.
File Growth	483 bytes.
Removal	Method 1.
Description	The virus contains the string `Kiev 1990`.

Kitty (None)

Type	Joke program.
Affects	N/A
File Growth	N/A
Removal	Method 3.
Description	Booting from an infected floppy causes display of either `We all love Kitty Bittersplit` or `Not a system disk (sorry)...`.

Kukac-Nagytud (Nagytud)

Type	Memory-resident file virus.
Affects	COM files on opening.
File Growth	448 bytes.
Removal	Method 1.
Description	The text `dv minden nagytud a naki Turbo @ ... ...` can be found near the end of infected files. This is similar to ***Kukac Turbo***.

Kukac Turbo (None)

Type	Memory-resident file virus.
Affects	COM files on opening, if smaller than 65,024 bytes long.
File Growth	512 bytes.
Removal	Method 1.
Description	The string `Turbo Kukac 9.9` can be found in the virus. If you press PrtSc, the above message is displayed repeatedly, resulting in a scrolling display.

Kylie (Jeru-Kylie)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except COMMAND.COM and before January 20th 1990 and after December 31st 1990.
File Growth	2,272 to 2,287 bytes.
Removal	Method 1.
Description	The string `Kylie Minogue` can be found in the virus. If a flag is set, the virus plays **Never Too Late**; however, there is nothing to set the flag. This appears to be a rewrite of ***Jerusalem***.
Variants	There are two versions; one is slightly corrupted and hangs the computer when it tries to infect.

Lazy (None)

Type	Memory-resident file virus.
Affects	COM files on execution, unless there is too much free space on the disk.
File Growth	720 bytes.
Removal	Method 1.
Description	The virus contains the text `[ lazy ]`. The screen display slows down to a crawl. The virus always goes memory-resident at 7000:A483, so if any other program uses that memory the computer will hang.

Leapfrog (V516)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	516 bytes.
Removal	Method 1.
Description	This virus is unusual in that it doesn't patch the jump command at the beginning of the file; instead, it patched the target of the jump. This makes it invisible to anti-virus programs which assume the jump is patched. The DOS version is occasionally reported as zero.

Leech (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. The virus is slightly polymorphic.
File Growth	1,024 bytes. This is concealed when the virus is memory-resident.
Removal	Method 2.
Description	The virus contains the text `The leech live ... April 1991 The Topler.` There is a 1 in 8 chance of seeing the message displayed and getting a two-sector overwrite on the hard disk.

Lehigh (None)

Type	Memory-resident file virus.
Affects	COMMAND.COM on execution of a program or when DOS looks for a file. The date/time is changed.
File Growth	None.
Removal	Method 2.
Description	The virus includes an infection counter which counts the number of times (not generations) the virus has replicated. When the virus creates a copy of itself, the counter is set to 0, and each time it replicates it increments the counter, which is then written back to the COMMAND.COM on the current disk. After the virus has copied itself four times it corrupts the disk by writing code from the BIOS to sectors 1 to 32. On a floppy disk this is difficult to recover from, as both copies of the FAT and the directory will be overwritten. On most hard disks this will not extend as far as the second copy of the FAT or the root directory, so it is easy to repair. After the overwriting, a string from the BIOS is displayed. This was probably the first documented PC virus. It originated at Lehigh University in the USA and has never been found in the field outside the USA.
Variants	Another version has a counter of ten, and has not been found outside the USA.

Leprosy (None)

Type	Overwriting file virus.
Affects	An EXE file in the current subdirectory on execution of an infected file. Some variants can infect COM files. Overwrites the first 666 bytes of a file.
File Growth	N/A
Removal	Method 2.

Description	Overwritten programs no longer work.
	
	There are two messages which may appear:
	
	`Program too big to fit in memory`
	
	or
	
	`NEWSFLASH! Your system has been infected with the incurable decay of LEPROSY 1.00 a virus invented by PCM2 in June of 1990. Good luck!`

Variants	**Leprosy-B:** The message is: `ATTENTION! Your computer has been afflicted with the incurable decay that is the fate wrought by Leprosy Strain B, a virus employing Cybernetic Mutation Technology(tm) and invented by T-PCM2 80.90` **Leprosy-C:** When an infected program is run it infects the next EXE program in the current subdirectory, overwriting the first 321 bytes. **Leprosy-D:** This infects both COM and EXE files, overwriting the first 370 bytes. There are no messages. There are also *e, f, g* and *h* variants, and ***Leprosy.Busted***. The *h* variant says `This program requires Microsoft Windows.`

Leszoptad (None)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks on booting from an infected floppy (installs itself on the hard disk) or hard disk (goes memory-resident and infects floppies).
File Growth	N/A
Removal	Method 3.
Description	**Hard disks:** the partition record is copied to (0,0,6). **Floppy disks:** the boot sector is copied to (0,1,3). On the 255th generation it displays `leszoptad!`.

Liberty (None)

Type	Memory-resident file virus.
Affects	An uninfected COM or EXE file on execution. Date/time and read/write attributes are preserved. Some versions also install on boot sectors.
File Growth	COM: 2,858 bytes to 2,868; EXE: 2,858 to 2,888.
Removal	Method 2, then Method 3.
Description	The virus contains the string `-MYSTIC-COPYRIGHT (C) 1989-2000, BY SsAsMsUsEsL`. There is no payload.
Variants	**Liberty.b** **Liberty.c**

Lisbon (648-Lisbon)

Type	File virus.
Affects	An uninfected COM file in the current directory on execution of an infected file, except those smaller than 10 and larger than 64,000 bytes. The **Abort, Retry, Ignore?** message is not disabled when write-protected diskettes are accessed.
File Growth	648 bytes.
Removal	Method 1. Files damaged by the 5-byte patch will need to be restored from a backup or the original.
Description	The virus uses the seconds field of the directory to store an impossible value of 62 seconds. One infection in four makes the file unusable. Eventually COMMAND.COM is infected, and then whenever the computer is started it hangs. It does this by putting the five characters `@AIDS` at the start of the file. This is a variant of ***Vienna***.
Variants	**Lisbon.b:** One file in eight is patched instead of being infected. When that file is run the computer hangs. **Lisbon.c:** This does not replicate except from the original file. **Lisbon.d:** This does not patch other files.

Little Pieces (None)

Type	Memory-resident file virus.
Affects	EXE files on execution.
File Growth	1,374 bytes.
Removal	Method 1.
Description	Every 30 keystrokes the screen is cleared and the cursor placed at the top left-hand corner. After this has happened eight times the message `One of these days I'm going to cut you into little pieces` is displayed. This is encrypted in the virus. The counter for eight times is never reset. The effects are not enabled until after a file has been infected.

Live after Death 1 (Phoenix 800)

Type	Memory-resident file virus.
Affects	COM files on execution, except COMMAND.COM and those larger than 64,512 bytes. Other file sizes are avoided, which means that about one file in eight is left alone.
File Growth	800 bytes.
Removal	Method 2.
Description	The string `Live after Death` is encrypted variably in the virus. Interrupt 13h is modified so that if a verify is requested it always returns OK. If a write is requested and the flags are set to failure, and read is done instead of the write. This is part of a long series from Bulgaria.

Live after Death 2 (V1226; Phoenix 1226)

Type	Memory-resident file virus.
Affects	COM files on opening, except COMMAND.COM and files larger than 63,488 bytes. There are other sizes it avoids, so about a file in 8 is left alone.
File Growth	1,226 bytes.
Removal	Method 2, then find out the extent of the FAT corruption. Re-install all software; some data files may also have been corrupted. Examine each file and restore a backup if necessary.
Description	The text is encrypted variably. The FAT is gradually corrupted by occasionally swapping two entries while they are in the sector buffer. This means that anything monitoring disk writes will fail to see the corruption, as it happens in memory, and DOS does the write. In addition, at the interrupt 13h level some disk reads are converted to writes. This is part of a series from Bulgaria.

Lovechild (None)

Type	Memory-resident file virus.
Affects	COM files on opening. Only works on MS-DOS 3.2. PC-DOS 3.2 systems hang.
File Growth	488 bytes.
Removal	Method 1, then delete any file which has been overwritten by the Trojan.
Description	The text `v2 (c) Flu Systems (R)` can be found in the virus. After 5,000 calls to interrupt 21h, when an EXE file is written there is a 75% probability that it will drop its Trojan as a replacement. The Trojan steps through the heads and cylinders of the hard disk, writing rubbish. It also displays the string `LoveChild in reward for software sealing`. The 'sealing' is presumably meant to be 'stealing'. If you try to create a file, there is a 3 in 16 chance that you will create a subdirectory instead.

Lucifer (Diamond-Lucifer)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,086 bytes. The increase is concealed.
Removal	Method 1.
Description	There is a video display, and the message `Lucifer (C) by C.J.` is displayed on Tuesdays. The video display shows on colour monitors exactly on each hour. A large multi-coloured diamond appears in the centre which then shatters into smaller diamonds that bounce around the screen until it is completely clear. This is one of the ***Cracker Jack*** viruses.

Magnitogorsk (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. EXE files must be bigger than 2,560, and COM files between 2,560 and 62,976 bytes.
File Growth	2,048 to 2,560 bytes. COMMAND.COM doesn't show the growth.
Removal	Method 1.
Description	If the virus is in memory, every time a program file is opened it is disinfected. Once an hour the following message is displayed: `Mr. Lozinsky ! Just read documentation on your AIDSTEST (1-Oct-90 version) we release new virus. Create improved versions of AIDSTEST to use it for out future designes, please ! Magnitogorsk, 3-Nov-90`
Variants	**Magnitogorsk-2048:** Files grow by 2,048 bytes. 36 minutes after going TSR the screen is inverted unless it is a mono character screen. Use Method 1.

Maltese Amoeba (Irish)

Type	Memory-resident file virus.
Affects	COM EXE files on execution. COM files must be between 450 and 63,000 bytes.
File Growth	2,498 to 2,565 bytes.
Removal	Method 2.

Description	The virus is polymorphic so is difficult for a scanner to detect. When decrypted, the poem inside is:
	
	`To see a world in a grain of sand,`
	`And a heaven in a flower`
	`Hold infinity in the palm of your hand`
	`And Eternity in an hour.`
	`THE VIRUS 16/3/91`
	
	The following text is also included:
	
	`AMOEBA virus by the Hacker Twins (C) 1991 This is nothing, wait for the release of AMOEBA II-The universal infector, hidden to any eye but ours! Dedicated to the University of Malta- the worst educational system in the universe,and the destroyer of 5X2 years of human life.`
	
	On November 1st and March 15th the Trojan is triggered on ATs and above. This overwrites the first four sectors, starting from (0,0,1), and repeats this on cylinders 1 to 29. This is repeated on all floppy drives. The next time the computer is started the poem is displayed.

Many Fingers (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,322 to 1,337 bytes.
Removal	Method 1.
Description	The virus contains the text `CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR.` This is displayed 1,500 keystrokes after infection, and the system is halted. This only happens on or after 11/11/1990.

Mardi (None)

Type	Memory-resident boot sector virus.
Affects	Hard and floppy disks on booting from an infected (not necessarily bootable) floppy.
File Growth	N/A.
Removal	Method 3.
Description	On floppy disks this uses sectors on track 41. The infected boot sectors contain `Sudah ada vaksin`, which is sometimes displayed, and the virus uses 7Kb of memory. There are similarities with ***Den Zuk***.

MG (None)

Type	Memory-resident file virus.
Affects	COM files on execution. A couple of other DOS interrupt function operations will also trigger infection.
File Growth	500 bytes. If the virus is in memory this is concealed.
Removal	Method 1.
Description	No effects.
Variants	***MG1***, ***MG2*** and ***MG3***. ***MG3*** does not infect files over 64,768 bytes long.

MGTU (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	273 bytes.
Removal	Method 1.
Description	There is a message in Cyrillic in the virus, and it has no payload.

Michelangelo (None)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks, when booted from and infected floppy. If the computer is booted from an infected hard disk the virus goes TSR and infects floppies in drive A:.
File Growth	N/A
Removal	Method 3.
Description	**Hard disks:** the partition sector is moved to (0,0,7) and the virus written to the original partition sector. **Floppy disks:** 360Kb: the boot sector is copied to (0,1,3). Others: the boot sector is copied to (0,1,14) which is the last directory sector of 1.2Mb floppies, and the last but one of 1.44Mb floppies. There is no such sector on 720Kb floppies. Every March 6th (Michelangelo's birthday), if the computer is an AT or PS/2, the Trojan is triggered. This steps through all heads and cylinders writing garbage to each track. On hard disks it assumes 4 heads, 256 cylinders, and 17 sectors per track. This is closely related to ***Stoned***.

Microbe (None)

Type	Memory-resident boot sector virus.
Affects	Floppy disks in drives A; or B: on reading or writing, when booted from an infected floppy.
File Growth	N/A
Removal	Method 3.
Description	The virus contains the text `This MICROBE is dedicated to 'Microchips Inc' Cebu City Phil. In appreciation for the quality training it provided us. 02/19/88 MICROMAGIC` The virus stores part of itself on track 39, head 1, sectors 2 to 9. This overwrites data on that part of the disk. A counter is incremented each time this happens, and when the count reaches 164 the display is triggered. The screen is cleared and the above message is displayed, then the computer boots normally. The virus's attempts to read the boot sector are redirected to the original boot sector, and fake bad sectors are created on the assumption that the diskette is a 360Kb floppy.

Migram (None)

Type	Memory-resident file virus.
Affects	EXE files on execution or opening.
File Growth	1,219 to 1,221 bytes. Only files between 1,221 bytes and 64Kb are affected.
Removal	Method 1.
Description	The virus contains the text `MIGRAM VIRUS 1.0 (C) 1991 IVL`. If a COM file is run, the first ZIP file in the directory is deleted. If an EXE file is run on a Saturday, tracks 0 to 5 on physical device 2 are formatted, and the message is displayed. However, physical device 2 is the third floppy drive so damage is unlikely. This is one of the ***Swami*** family.
Variants	**Antichrist:** Files grow by 1,008 bytes, and the virus contains the text `*.ZIP`. Whenever a file is infected the virus tries to delete the first ZIP file in the subdirectory. **Migram-Cemetery (Cemetery):** Both COM and EXE files are infected on opening and execution, growing them by 1,417 bytes. It avoids files called *ND.* such as COMMAND.COM. The virus contains the word `CEMETERY`, and at 4pm a display is triggered. At times outside 4pm to 5pm, if a '1' is input to the serial port the computer is rebooted.

cont...

	Migram-Smack (Smack): Both COM and EXE files are infected on opening and execution, and grow by 1,835 bytes. Files conforming to *ND.* (such as COMMAND.COM), *AN.* (many scanners have such names), *HA.* and *HK.* are avoided. The virus contains the text `This virus was written in Italy by Cracker Jack 1991 IVRL All rights reserved, please don't crack this virus!!`. There is also an insult to a lady virus researcher. When an EXE file is run on a Friday, the question `Is today Friday? (Y/N)` is displayed. Answering Y or y produces the response `Sorry but on Friday I wish not work!!` and a quit to DOS without letting the host program run. If the answer is anything else, the response `You are untruthful!! For punishment I format your HD Fat!!`. It then formats track 0 head 0 of the third floppy drive five times. This is probably meant to be damaging the hard disk but is miscoded. There are a lot of NOP instructions in the code for going memory-resident, perhaps to fool scanners.

Minsk-1075 (Russ-1075)

Type	Memory-resident file virus (faulty).
Affects	Intended to infect COM and EXE files.
File Growth	Would add 1,075 bytes if it worked.
Removal	Method 2.
Description	This is intended to corrupt DBF files, but is too faulty to function. Some of the interrupt 21h calls are coded as interrupt 21 calls.

Mirror (None)

Type	Memory-resident file virus.
Affects	Uninfected EXE files on execution or opening.
File Growth	924 to 940 bytes
Removal	Method 1.
Description	After ten minutes the display is changed left for right, producing a mirror image of what should be there.

Mix1 (Mixer1)

Type	Memory-resident file virus.
Affects	EXE files on loading when larger than 8,192 bytes. Read/write attributes are preserved. The memory-resident part of the virus is in high conventional memory and uses 2,048 bytes. The **Abort, Retry, Ignore?** message is not disabled, so the correct message is given if a write-protected diskette is accessed.
File Growth	1,618 bytes.
Removal	Method 1.

Description	The most obvious effect is the garbling of serial and parallel port information, affecting modems, printers, mice etc. Numbers are unaffected, and the following table is used to translate characters:
	
	`abcdefghijklmnopqrstuvwxyz`
	`ebsdapghejklmnufqrctovwxyz`
	
	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
	`BECDAPGHYJKLMNUFQRSTOVWXIZ`
	
	For example, **Bad command or file name** becomes **Eed summend ur pela nema**.
	
	A counter increments every time a file is infected after the virus goes memory-resident, and is written to every infected file. If the count is greater than 5, 60 minutes later a bouncing ball is displayed (lower case o) which bounces of the sides of the screen. It is not deflected by letters (unlike ***Italian***) but replaces letters over which it passes. After 50 minutes the keyboard handler is replaced with a routine which always turns off Caps Lock and turns on NumLock. If the computer is then rebooted the bouncing ball is displayed.
	
	This virus is modelled on ***Icelandic***.

cont...

Variants	**Mix1-b:** The files grow a little more. **Mix 2:** This infects COM and EXE files, which grow by 2,280 bytes. The last 4 bytes of infected files are `MIX2`, and the virus contains the strings `Strike the pauseVogue, you got to Let your body move with the music` and `I can leave you, say goodbye, i can love u if i try.....Left to my own devices i probely could`. This is encrypted and not displayed. The first string is from a Madonna album, and the second is from a Pet Shop Boys album. The garbling effects are similar to ***Mix1***. When Ctrl Alt Del is pressed, all characters on the screen are incremented or else NOTted. 48 minutes after going memory-resident the screen trick is triggered.

Month 4-6 (Agiplan)

Type	Memory-resident file virus
Affects	COM files on execution, except COMMAND.COM. Only files smaller than 56Kb are infected.
File Growth	1,536 bytes.
Removal	Method 1.
Description	If a file is run four months after being infected, some disk writes are corrupted. If a file is run after six months, the first five cylinders, all heads and sectors 1 to 9 on drives A: to D: inclusive are trashed.
Variants	There are two variants: ***a*** and ***b***.

Monxla (None)

Type	File virus.
Affects	A COM file in the same subdirectory or one referred to in the path on execution of an infected file. Only files between 3,840 and 64,000 bytes are affected.
File Growth	939 bytes.
Removal	Method 1.
Description	The text `(C) Monxla` can be found at the end of infected files. On the 13th there is a 40% chance that instead of infecting a file, the virus will patch the start with a HALT command, which stops the computer when the program is run. There is a 30% chance that it will patch it with an interrupt 19h, which on some computers causes a reboot and others hangs the system. This has a strong relationship to ***Vienna***.

Mosquito (None)

Type	Memory-resident file virus.
Affects	EXE files on execution.
File Growth	1,025 to 1,040 bytes.
Removal	Method 1.
Description	The virus contains the encrypted text `WorZ a stopHello this is the core Rev 3 26/4/91 P 0.98c P.0.98 Rev 4 24IX89 bye bye` . the word **Mosquito** is unencrypted. On the 25th and 26th, if an infected program is run the virus generates a critical error and the DOS message **General failure reading drive x** is displayed.
Variants	***FaxFree***

Mule (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. EXE files are repeatedly infected.
File Growth	COM: 4,117 bytes; EXE: 4,112 to 4,127 bytes.
Removal	Method 1.
Description	The virus contains `Mule .` near the beginning. On Friday 13th the first infected program run displays the message `My name is Mule. It's a good time.` and hangs the computer. This virus is from the ***Jerusalem*** family.

Murphy (Murphy-1; Murphy-2; 10 AM)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution and copying, except those smaller than the virus itself and those set to read-only. COMMAND.COM is infected immediately, so control is taken as soon as the computer is booted. Date/time are preserved.
File Growth	**Murphy-1**: 1,277 bytes. **Murphy-2:** 1,521 bytes.
Removal	Method 1.
Description	Disk error messages are disabled, but because of bugs in the code the **Abort, Retry, Ignore?** message may be displayed several times if the virus tries to write to a write-protected disk. Both variants trigger when the system clock reads any time between about 10am and 11am. **Variant 1:** causes the speaker to whistle at a high frequency and crackle when keys are pressed or a program run. The crackle stops when the time is changed to after 11am, but the whistle continues. **Variant 2:** a dot (ASCII 07, the small diamond shape) to bounce around the screen, off the edges of the screen and any displayed characters. It doesn't usually corrupt text, but occasionally leaves a trail of dots on the screen and moves a few existing characters when the screen scrolls. The dot continues after the time changes. Neither variant deliberately damages data other than infecting executable files.

cont...

Variants	**Murphy-1:** As well as the effects above, this contains the message `Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofi, USM Laboratory.` **Murphy-2:** As well as the effects above, this contains the message `It's me - Murphy. Copywrite (c)1990 by Lubo & Ian, Sofi, USM Laboratory.` **Murphy-3:** As *Murphy-1*, but files grow by 1,284 bytes. **Murphy-4:** As *Murphy-2*, but files grow by 1,480 bytes.

Musicbug (None)

Type	Memory-resident boot and partition sector virus.
Affects	Floppy (drives A: and B:) and hard disks when booted from an infected floppy disk.
File Growth	N/A
Removal	Method 3.
Description	**Hard disks:** the partition sector looks normal, but at the place where the virus begins is the text `MusicBug v1.06. Macrosoft Corp.` and near the end is `-- Made in Taiwan --`. **Floppy disks:** these have 4Kb in lost clusters, which are used to store the virus. When the virus is in memory it uses stealth techniques to hide. The virus plays a random tune.

Natas (None)

Type	Memory-resident file, boot and partition sector virus (multipartite).
Affects	Fast infector: COM and EXE files on execution or close (e.g. when copying – both source and destination). COM files longer than 60,692 or shother thatn 1,000 bytes and EXE files longer than 938,040 bytes are not infected. The hard disk's partition sector is infected when an infected program is executed, or when booted from an infected diskette. Floppy disks are infected on read access (e.g. DIR command).
File Growth	4,744 bytes.
Removal	Files: Method 1. Boot and partition sectors: Method 3.
Description	The virus in infected files is variably encrypted and polymorphic. The virus demonstrates full stealth – when it is active in memory it conceals all changes to infected files and disks. Unlike most full stealth viruses, ***Natas*** can survive archiving (ARJ, LHArc, PKZip), backups (BACKUP, PCBACKUP) and transfers of infected files via modem (ZMODEM, XMODEM etc.). It does not trigger CHKDSK file system error reports. When booted from an infected hard disk, approximately one in 512 times the virus triggers and formats all hard disks in the system, destroying all data on them. The virus can also trigger when being traced with a debugger. It contains the encrypted strings `Natas`, `BACK` and `MODEM`.

Necropolis (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,963 bytes. This is concealed. One cluster is added to the FAT chain of files without changing the directory entry; this is used to store the extra code. If the virus is in memory, files look normal to a DOS read.
Removal	Method 2.
Description	This virus makes extensive use of tunnelling, going under interrupts 21h and 13h when it writes to disk, ensuring that generic monitoring programs can't detect the writes. Most DOS functions are trapped and redefined to achieve the stealth effect.
Variants	**Necrophylia-b:** Forty bytes have been patched to put in the message `(C) by Cracker Jack 1991 - IVRL NeCrOpHyLiA.` This variant does not function properly.

Nina (Happy New Year 1600; V1600)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COMMAND.COM and SYS files are avoided.
File Growth	1,600 bytes. EXE files vary from this slightly.
Removal	Method 1.
Description	The virus contains the text `Dear Nina, you make me write this virus; Happy new year!`. Whenever a file is written to, the boot sector is read, one word is changed at offset 3 (the OEM label) and then written back. This appears to be a rewrite of ***Jerusalem***.

Nina 2 (Nina-256)

Type	Memory-resident file virus.
Affects	COM files on execution, except those between 500 and 65,200 bytes long and those set to read-only.
File Growth	256 bytes.
Removal	Method 1.
Description	The virus contains the text `Nina`, and has no payload. It is completely different from ***Nina***.

NJH (LBC; Korea; NJH-LBC)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks, when booted from an infected floppy disk. Memory is reduced by 2Kb at the top.
File Growth	N/A
Removal	Method 3. On hard disks, the original boot sector will have overwritten one of the FAT sectors, so you must use a disk sector editor to copy the good version of the sector from the second copy of the FAT to the first. If this is not possible, do a low-level format, partition it with **FDISK** then **FORMAT** it with the **/S/V** switches. Check the disk again with **FindVirus** and restore the most recent backup.
Description	Infected boot sectors contain the text `virse program messge Njh to Lbc.` The virus replaces the boot sector with its own code and moves the original boot sector further up the disk. On a hard disk it moves the partition sector. No intentional damage is done, but because the place where the original boot sector is stored doesn't vary with the type of disk, problems occur on disks of capacity greater than 360Kb. There is a test in the virus to avoid infecting hard disks, but it doesn't work. The original partition sector is copied over part of the first copy of the FAT, making the hard disk inaccessible Floppy disks are inoculated against ***Brain*** and ***Ping Pong***.

No Bock (None)

Type	File virus.
Affects	Random number of COM files on execution of an infected files, provided they are between 2,000 and 64,000 bytes long.
File Growth	440 bytes.
Removal	Method 1.
Description	If a file is run nine months after it is infected, the message `No Bock today Error, System halted!` is displayed and the system hangs.

Nomenklatura (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution if they are larger than 1,024 bytes. COM files must less than 64,000 bytes.
File Growth	1,024 bytes.
Removal	Method 1.
Description	The virus contains the text `Nomenklatura`. The FAT is gradually corrupted by swapping words in the memory copy of the FAT where there are long FAT chains (which means large files). DOS then writes the memory copy of the FAT to disk as normal. This is done so that monitor-type programs cannot prevent the corruption. There are a number of similarities to the ***Live after Death*** series, for example in the payload code. The damage done by ***Nomenklatura*** is gradual and subtle, which means that it could be a long while before it is discovered, by which time the corrupted files have been backed up many times.
Variants	**Nomenklatura.b:** Because of a corruption in the code, if it tries to infect an EXE file it causes system problems such as **Divide by zero**, or the system hangs.

Noon-beep (Milous)

Type	Memory-resident file virus.
Affects	COM files on execution. Files must be between 32 and 62,464 bytes long.
File Growth	1,163 bytes.
Removal	Method 1.
Description	At 12 noon, the speaker gives three short beeps and a long one. The virus contains a routine to remove itself from files.

Number of the Beast (NotB; V512; 666)

Type	Memory-resident file virus.
Affects	COM files on execution of any of a number of DOS functions such as copying, executing or reading. Read/write attributes and date/time are preserved.
File Growth	Apparently none. The virus is inserted into unused space at the end of the cluster.
Removal	Method 2. It is very important to boot from a clean DOS disk as this virus can conceal itself completely from any anti-virus program and is memory-resident.
Description	This virus hides itself very well, but some DOS utilities may give inappropriate error messages. There is no payload. It appears to have been written as an exercise in using the internals of DOS. However, an infected file will only work if it is copied after the virus goes memory-resident; if it is copied before, the copy won't work, but the virus will still go TSR and infect subsequent programs. The virus hides itself in memory so that it is invisible to most memory map programs and monitors. The virus identifies files it has already infected by changing the seconds field in the timestamp to 62 seconds, although this is not visible when inspected using **DIR.** This virus has been written by an extremely cunning author and uses many undocumented features of DOS. It is signed `666` at the end, hence the name.
Variants	There are 13 variants which are functionally identical, differing only in implementation of the code.
	Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS diskette, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will *NOT* be seen by DOS. For this reason, it is strongly recommended that the Anti-Virus Toolkit be used from the original write-protected floppy disks until the virus has been eradicated.

Number One (Burger-Pascal)

Type	Overwriting file virus.
Affects	A COM file in the same directory on execution of an infected program.
File Growth	None. Overwrites the first 12,032 to 13,952 bytes.
Removal	Method 2.
Description	The virus contains the string `This file has been infected by Number One`. If all files have been infected the message `<smile>` is displayed. This virus was first published in the Burger book in Pascal source code.
Variants	**Number 1.b:** Each infected program announces itself by displaying `The Fie Has Been Infected by Number One`.

NYB (New York Boot, B1)

Type	Memory-resident boot sector virus.
Affects	Hard and floppy disks on booting from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	Although badly written, this simple stealthing boot sector virus is commonly found in the wild. The original uninfected boot sector is moved to 0,0,11 on hard disks, and to the last sector of the root directory on floppies.

Ogre (Computer Ogre; Disk Killer; Disk Ogre)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks, when the machine is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.

Description	If an infected computer is left on for 48 hours and the hard disk is accessed during the next hour, the virus is triggered. The screen clears and displays:
	
	`Disk killer - Version 1.00 by COMPUTER OGRE 04/01/1989`
	
	`Warning !!`
	
	`Don't turn off the power or remove the diskette while Disk killer is processing!`
	
	`PROCESSING`
	
	An infected computer loses 8Kb of memory, and infected diskettes have 3Kb of bad sectors.
	
	Floppy disks: the boot sector is moved up the disk and replaced. Because the wrong group of sectors is marked as bad, *Ogre* leaves itself vulnerable to being overwritten by data placed on the diskette later.
	
	Hard disks: the boot sector is moved up the disk and replaced. When the virus is triggered it encrypts the contents of the bootable disk partition.

Variants	There is a version where the message contains `Version 1.04`.

Old Yankee (None)

Type	File virus.
Affects	EXE files on execution of an infected file.
File Growth	Two versions: 1,961 and 1,624 bytes.
Removal	Method 1.
Description	The virus plays Yankee Doodle when an infected program is run. This is very different from ***Yankee Doodle*** which also plays Yankee Doodle.

Omega (Friday-13th-440)

Type	File virus.
Affects	COM files in every subdirectory and on drive C:, on execution of the infected file.
File Growth	440 bytes.
Removal	Method 1. If the payload has triggered it will be necessary to replace the boot and partition sectors, then copy those FAT sectors which have been overwritten from the second copy of the FAT. This should be done carefully by hand – an automatic disk-mending program might not do it correctly.
Description	When an infected program is run there is a lot of disk activity as each COM file on the hard disk is read to see if it is already infected. On every Friday 13th the payload is triggered. This overwrites the hard disk, cylinder 0, head 0, sectors 1 to 8, with garbage; then cylinder 0, head 1, sectors 1 to 8. The first overwrite hits the partition sector, and the second will overwrite the boot sector and part of the FAT on most computers. This is one of several viruses called ***Friday 13th*** – see also ***Virus-B*** and ***Jerusalem***.

ON 64 (V696)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	696 bytes after padding to a multiple of 16 bytes..
Removal	Method 1.
Description	After 64 infections the Trojan triggers, overwriting the first four heads of cylinder zero of the hard disk.

One Half.3544 (Free love)

Type	Memory-resident file and partition sector virus (multipartite).
Affects	Fast infector. Infects COM and EXE files on execution, open, rename etc. The partition sector of the hard disk is infected when an infected program is executed.
File Growth	3544 bytes.
Removal	Method 1.

Description	The virus in infected files is variably encrypted and polymorphic.
	
	The virus demonstrates stealth capabilities – when it is active in memory, it conceals all changes to the infected hard disk partition sector and any growth in file size.
	
	The partition sector is infected when an infected program is executed. COM and EXE files are infected on virtually any access to them – it is a fast infector.
	
	The nastiest feature of ***One Half*** is its payload. When a hard disk is infected, the virus calculates the position of the last cylinder of the last DOS partition. Every time the computer is booted, the virus encrypts two cylinders, starting from the last two and moving towards the beginning of the partition. The pointer to the last encrypted cylinder is updated in the infected partition sector. When the pointer falls below approximately one half of the total number of cylinders (i.e. when half the hard disk partition is encrypted) the virus triggers, provided the date is a multiple of 4. When this happens the virus displays the message:
	
	`Dis is one half`
	`Press any key to continue.....`

Variants	There is a variant 3577 bytes long.

Ontario (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. COMMAND.COM is infected straight away, and COM files must be smaller than 57,335 bytes.
File Growth	COM: 512 bytes; EXE: 536 to 688 bytes.
Removal	Method 2.
Description	There is no payload.

Oropax (Music virus; Musician)

Type	Memory-resident file virus.
Affects	The next COM file in the current subdirectory when a subdirectory is created or removed, or a file is created, opened for writing, deleted or renamed. COMMAND.COM is avoided.
File Growth	2,756 to 2,806 bytes to a multiple of 51.
Removal	Method 1.
Description	One in four times, five minutes after the virus goes TSR it plays one of three tunes every seven minutes. These are: • The Stars and Stripes For Ever • Mozart Symphony No. 40 • Blue Danube ***Oropax*** is a brand of German earplugs.

Paris (TCC)

Type	File virus.
Affects	An uninfected COM or EXE file on execution of an infected file.
File Growth	4,909 to 4,934 bytes. COM file must be smaller than 58,368 bytes to be affected.
Removal	Method 1.
Description	The virus fails to work correctly on hard disks with capacities other than 10 or 20Mb.

Parity (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	441 bytes.
Removal	Method 1.
Description	When an infected file is run, there is a 3% probability that the message `PARITY CHECK 2 2000 (S)` will be displayed and that the computer will hang.

Parity boot (None)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks.
File Growth	N/A
Removal	Method 3.
Description	This stealth boot and partition sector virus can survive a warm boot (Ctrl Alt Del). When booted from an infected disk, the virus stays memory-resident and infects hard and floppy disks being read (e.g. via the DIR command). If an uninfected floppy is write-protected, the virus will perform an infinite loop when trying to infect it, hanging the computer. The virus demonstrates stealth techniques, concealing changes made to boot and partition sectors. If no disks are infected during approximately one hour, the virus triggers and on the next keystroke displays the message: `PARITY CHECK` and hangs the computer.
Variants	There are three slightly different variants.

PcVrsDs (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	1,904 bytes. EXE files are rounded to a multiple of 16 bytes. The increase in concealed from **DIR** when the virus is in memory.
Removal	Method 1.
Description	Encrypted inside the virus is the text `PcVrsDs Version 1.00 Copyright (C) VirOP 1990.` In 1990 the virus infects 16 files and then deletes any file run or opened. In 1991 or after, this happens after 6 infections. On Monday (but not in 1990, or on the 23rd), the virus waits for 255 keystrokes, then every 14th keystroke is altered to produce the next higher ASCII character. On the 23rd (but not a Monday) programs infected that day will not run later on, unless the virus is already in memory when you try to run them. Ten days after any Friday 13th the payload is triggered. This does a low-level format of the hard disk, tracks 0 to 31 head 0. The message is then displayed. There is a strong resemblance to ***Jerusalem***, but the differences are substantial.

Perfume (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Read-write attributes are preserved.
File Growth	765 bytes.
Removal	Method 1.
Description	When infecting a file, four bytes are added at the end. The first two of these are the self-recognition code **VI**, and the second two are a counter initialised to 0. Every time the file is run the counter is incremented, and when it reaches 80 a message is displayed before the program is run. If **4711** is typed in response to the message, the program continues; typing anything else produces a second message and the program terminates with a return code of 1, which is an error level usually produced by abnormal termination (crashing). In one sample the message is replaced by nulls. 4711 is a famous perfume.
Variants	**Perfume-731:** COM files grow by 731 bytes. The messages are intact; the first is `Bitte gebe den G-virus Code ein`, and the second is `Tut mir Leid` (Sorry). ***Perfume.blank, Perfume.message, Perfume.Slash***

Phoenix phoenix (Live after Death 4)

Type	Memory-resident file virus.
Affects	COM files on execution. Some sizes are avoided so about one in eight will be left alone.
File Growth	1,704 bytes; COMMAND.COM is infected without growth.
Removal	Method 2. You will have to find the extent of corruption introduced by the FAT changes. Each file should be examined and the backup restored if necessary.
Description	The virus contains the encrypted text `PHOENIX`. The encryption and decryptor/loader are variable. The FAT is slowly corrupted by occasional swapping of two entries in the sector buffer; anything monitoring disk writes fails to see the corruption as it happens in memory before DOS does the write. At interrupt 13h level some reads are converted to writes and some EXE files Trojanised.

Ping Pong (Italian; Ping Pong-B; Bouncing Ball; Mistake; Bouncing dot; Vera Cruz; Turin)

Type	Memory-resident boot sector virus.
Affects	Hard and floppy disks on 8086 and 8088 (XT) machines when the machine is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	Once every 30 minutes, if the disk is being accessed, a bouncing dot on the screen is triggered. Infected diskettes have one cluster (1Kb or 512 bytes) of bad sectors; hard disks lose one cluster (usually 2Kb). This virus replaces the boot sector of a disk with its own code and moves the original boot sector further up the disk. The virus has no ill effects other than slowing down the floppy drive and making 2Kb of memory unavailable to DOS.

Variants	**Big Italian:**
	This generates a diamond shape instead of a dot and *will* infect 80286 and 80386 machines.
	
	Mistake (Typo; Typoboot):
	This exchanges characters while they are being output to the printer, using the following substitution table:
	
	`18CKGJMNOU36VW27ckgjmnou49vw`
	
	1 is substituted for 8 and vice versa, C for K and so on. It also does a substitution on some of the high-order bytes:
	
	`80h 92h 9Ah 88h 97h 8Bh 85h 8Fh`
	
	This is more meaningful when the Hebrew character set is used.
	
	NOTE: the ***Fumble*** virus, which is quite different, is also sometimes called ***Typo***.

Piter (None)

Type	Memory-resident file virus.
Affects	COM files on execution, if they are between 2,000 and 64,000 bytes long.
File Growth	529 bytes.
Removal	Method 1.
Description	The first time an infected program is run without the virus in memory, the virus goes TSR and the program doesn't run.

Pixel (None)

Type	File virus.
Affects	All COM files in the current subdirectory on execution of an infected file. DOS write-protect error messages are not suppressed for floppies.
File Growth	Varies according to the version (see below). Date/time and read/write attributes are preserved in some and not others.
Removal	Method 1.
Description	The virus has counter which keeps track of the generation number. After the fifth generation there is 50% probability of getting the message `Program sick error:Call doctor or buy PIXEL for cure description` when an infected file is run. This virus was allegedly published in a Greek computer magazine in BASIC; when this program is run it creates a COM file which is the virus. It reached Bulgaria in this form and was then worked on by various programmers to create new versions.
Variants	These versions are all nearly functionally equivalent to the original, but seem to have been attempts to reduce the byte-count of the virus. **Pixel-905:** As ***Pixel-897***, but only on or after the third generation. **Pixel-899:** As ***Pixel-897***. **Pixel-899b:** Formats the third floppy drive, if present. **Pixel-897:** Looks for dates on or after April 1st, when there is a 50% chance of the payload triggering. This displays the message and formats drive A: track 0 head 0.

cont...

	Pixel-892: After the third generation, as ***Pixel-905***, but the message is obscene. **Pixel-877:** On the ninth generation the message `Sector not found error fucking defoult drive! Please buy me a new disk drive!` is displayed. **Pixel-854:** The message is in Cyrillic. **Pixel-850:** As in the description above. **Pixel-847:** This is the original version. The self-recognition code is **VI** in bytes 3 and 4 in the file. Read-only files are not infected. **Pixel-837:** The message is `I love you so much!!! -- Francis.` **Pixel-779:** As in the description above. **Pixel-345:** This corrects the major bug in ***847*** which meant that what was copied was far too long. The self-recognition code is now at bytes 2 and 3. **Pixel-299:** Date/time are preserved, and it uses the Disk Transfer Area instead of defining a local one, which reduces byte-count.

cont...

Pixel-295:
As in the description above.

Pixel-283:
Triggers at the 16th generation. The message is `What a stupid you are !!!!!!!!`.

Pixel-277 (V-277):
The message is absent and replaced by a beep which never happens because of a bug in the code which tests for a 50% chance to do it. The self-recognition code is **UM** in bytes 2 and 3.

Pixel-275:
Triggers at the second generation. The message is `Fucking hell:You wet pussy`.

Pixel-Year-6545:
Files grow by 936 bytes. On April 1st year 6545 and thereafter the virus displays a message and formats track 0 of a floppy in drive A:. The message starts with some obscenities, then continues `HaHaHa... What a Good Friday!!`. The year is because of a bug which confuses hex and ASCII.

Nocargar:
This is ***Pixel-847*** with the message changed to `En Tu PC hay un virus RV1, yesta Es su quinta generacion.`

Luz (Advert):
Files grow by 847 bytes and the date/time is not preserved. The message is changed to `Hello, John Mcafee,please uprade me.Bests regards,Jean Luz.`

There are further versions which grow files by 740 and 257 bytes.

Plague (None)

Type	Overwriting file virus.
Affects	COM and EXE files on execution of an infected program.
File Growth	None. Part of the code is overwritten.
Removal	Method 2.

Description	Infected programs no longer work, but display the message `Program too big to fit in memory`. if there are at least eight infected files and there are no more left to infect, the message:
	
	`Autopsy indicates the cause of death was`
	`THE PLAGUE Dedicated to the dudes at`
	`SHHS VIVE LE SHE_MAN!`
	
	Is displayed and the current drive is trashed by overwriting a random number of sectors, starting with the boot sector.
	
	Whichever message it gives, the keymatic repeat rate is reprogrammed on AT machines, setting the delay to one second and the rate to two characters per second.

Variants	This is similar to ***Leprosy***.

Polimer (None)

Type	File virus.
Affects	A COM file on execution of an infected program.
File Growth	512 bytes.
Removal	Method 1.
Description	Files contain the text below near the start. When an infected file is run, the message `A le'jobb kazetta a POLIMER kazetta ! Vegye ezt !` is displayed. If there is a read or write error during the infection it displays `ERROR`.

Possessed (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except COMMAND.COM.
File Growth	2,367 bytes. EXE are rounded up to the nearest multiple of 16 bytes.
Removal	Method 1.
Description	The virus contains the string `POSSESSED! Bwa! ha! ha! ha! ha! Author: JonJon Gumba of AdU.` If 2,400 bytes or less are available on the drive, or a COM file contains the self-recognition code without being infected, the virus deletes programs instead of infecting them. Three hours after the virus goes memory-resident, the screen switches to graphics mode and a cartoon of a devil's face with horns is displayed in the centre and shaken and wobbled around.
Variants	**Possessed.b:** This adds 2,446 bytes to files. The text string has `Fucker.` added to it. The screen display happens four hours after the virus goes resident.

Print Screen-1024 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files between 1,024 and 64,512 bytes are affected.
File Growth	1,024 bytes.
Removal	Method 1.
Description	This randomly causes a screen dump to the printer. If no printer is attached, this may appear to cause a slowdown, or almost a halt, of computer operation, as the system will wait for a timeout on the printer before proceeding.

Print Screen Boot (None)

Type	Memory-resident boot sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	This triggers a print-screen every now and then, and uses 2Kb of memory. If no printer is attached, this may appear to cause a slowdown, or almost a halt, of computer operation, as the system will wait for a timeout on the printer before proceeding. Boot sectors are replaced and the original boot sector moved further up the disk. There are a number of bugs in the virus, as the author has assumed that all hard disks are laid out as a 4-head, 17 sector-per-track, 20Mb disk under DOS 3. With a disk of any other geometry the virus could overwrite any part of the disk, including the FAT, when it moves the boot sector. The same problem can occur with floppies as the virus assumes then to be 360Kb. This virus appears to derive from three older viruses: ***Brain***, ***Italian*** and ***Stoned***.

Proud (Live after Death 5; Phoenix Proud)

Type	Memory-resident file virus.
Affects	COM files on execution. Some sizes are avoided so that about one file in eight is left alone.
File Growth	1,302 bytes. COMMAND.COM is infected without growth.
Removal	Method 2. You will have to find the extent of corruption introduced by the FAT changes. Each file should be examined and the backup restored if necessary.
Description	The text `Proudly made in Sofia` is encrypted in the virus. The encryption and decryptor/loader are variable; the virus is polymorphic. The FAT is gradually corrupted by occasionally swapping two entries while they are in the sector buffer. This means that anything monitoring disk writes will fail to see the corruption, as it happens in memory, and DOS does the write. In addition, at the interrupt 13h level some disk reads are converted to writes. This is part of a series from Bulgaria.

Prudents (1210)

Type	File virus.
Affects	The next EXE file on execution of an infected file. Date/time are not preserved. If the subdirectory name has an extension, files within it and lower down the tree will not be infected.
File Growth	1,205 to 1,230 bytes.
Removal	Method 1.
Description	The virus contains the encrypted message `# Prudents virus. Barcelona 2028289 #` which is decrypted when the virus runs, but not displayed. If the year is not 1989, the month is between May and December, and it is the 1st, 2nd or 3rd, the payload is installed. This converts every write to the disk to a verify so that it appears as if the write is successful whereas it hasn't actually happened. This applies to both floppy and hard disks. If the virus can't open a file, or if an EXE files doesn't have the required MZ at the start, it deletes the file. There is another payload in the virus which is never called, which does a low-level format of the hard disk. This is concealed from programs which search for such code by using a run-time patch to complete the interrupt code.

Quit-1992 (555; Dutch-555)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	555 bytes.
Removal	Method 1.
Description	If the year is 1992 or later, infected programs do not run.
Variants	**Quit-1992.B:** This has the same effects, but there is a minor difference in the code.

Quox (Stealth)

Type	Memory-resident boot and partition sector virus.
Affects	Floppy and hard disks.
File Growth	N/A
Removal	Method 3.
Description	This stealth boot and partition sector virus has no intended payload. When booted from a hard disk, the virus stays memory-resident and infects hard and floppy disks being accessed (e.g. via the DIR command). The virus demonstrates stealth techniques, concealing changes made to boot and partition sectors. Since the virus uses some 80286-specific instructions, it will not operate properly on pre-80286 computers (most XTs).

Raubkopie (None)

Type	File virus.
Affects	A COM or EXE file on execution of an infected file.
File Growth	COM: 2,219 bytes. EXE: 2,476 to 2,491 bytes.
Removal	Method 1.
Description	The messages are encrypted. A message in German is displayed asking for a **J/N** (Yes/No) response. If you type [N] it displays two more messages in German and exits. If you type [J] it displays one message and continues. Next, if it is after 6pm on the 15th, it installs a keyboard trick. If it is Friday 13th it tries to overwrite the partition record, but fails because of a bug in the code.

Ray Joke (None)

Type	No replication.
Affects	N/A
File Growth	N/A
Removal	Delete the file using the DOS **DEL** command.
Description	When run, this displays the message `Run it again, Ray` and creates a file called RAY.COM. When that is run it displays `How was this done, Ray?`.

RC-1049 (USSR-1049)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. EXE files are grown but not actually infected.
File Growth	1,049 bytes after rounding to a multiple of 16.
Removal	Method 1.
Description	There is no payload.

Red Diavolyata (Iskey; MLTI)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	662 to 830 bytes.
Removal	Method 1.
Description	The text `Eddie die somewhere in time!` can be found near the end of the file, which is perhaps a reference to ***Dark Avenger***. Another message is `The programm was written in the city of Prostokwashino (C) 1990 RED DIAVOLYATA Hello! MLTI!`. On Fridays, three hours after the virus goes TSR, every program run is deleted instead.

Revenge (None)

Type	Memory-resident file virus.
Affects	COM files whenever the user changes directories.
File Growth	1,127 bytes.
Removal	Method 1.
Description	The virus contains the text `*** 777 - Revenge Attacker V1.01 ***`. When it triggers, it overwrites drives C: and D: seven sectors at a time, starting with the boot sector. For each seven sectors overwritten a '7' is displayed on the screen.

Ripper (Jack Ripper)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 1.

Description	This virus can be very destructive. On every write operation it performs a logical AND operation with the timer tick count and 3FFh. If the result is zero, it swaps randomly-chosen bytes in the write buffer. This has the effect of corrupting information as it is written to the hard disk. On average, this corruption occurs once in every 1024 writes.
	
	This makes it very hard to detect damage to data. Instead of wiping the disk outright, which the user would notice immediately and fix by restoring a backup, ***Ripper*** makes small corrupting changes which are not noticed. By the time the problem is discovered, the backups themselves are also corrupted.
	
	The virus contains the following encrypted messages which are never displayed:
	
	`FUCK 'EM UP !`
	
	and
	
	`(c)1992 Jack Ripper`

Russian Mirror (Beeper)

Type	Memory-resident file virus.
Affects	Every third COM file on execution.
File Growth	482 bytes.
Removal	Method 1. If the Trojan has triggered, **CleanPart** *may* be able to repair the damage.
Description	After one thousand calls to interrupt 21h the Trojan triggers. The computer beeps as the screen image is swapped left for right (making a mirror image), then the partition sector is overwritten with rubbish.

Sadam (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, opening, renaming, creation and when various other DOS functions take place.
File Growth	919 bytes.
Removal	Method 1.
Description	With one infection in eight, the message `HEY SADAM LEAVE QUEIT BEFORE I COME` is displayed. This has a strong resemblance to ***Stupid***.
Variants	***Queit, Profesor***

Sampo (Turbo, W1lop)

Type	Memory-resident boot and partition sector virus.
Affects	Write-enabled hard and floppy disks if the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 1.
Description	This boot and partition sector virus infects the partition sector of the hard disk when booted from an infected floppy. It then infects floppies on read access (e.g. the DIR command). When active in memory, the virus will stealth the infected partition sector, but not floppy disk boot sectors. It can survive a warm boot (Ctrl Alt Del). If a write-protected diskette is accessed on an infected computer, the virus fakes the boot sector to look as though it is infected with ***Telefonica.A*** using a stealth-like mechanism. This can cause ***Telefonica*** false positives on a ***Sampo***-infected PC. On the 30th November, approximately two hours after the PC was booted, the virus triggers and displays the following message: SAMPO "Project X" Copyright (c)1991 by the SAMPO X-Team. All rights reserved. University Of The East Manila

Satan Bug (None)

Type	Memory-resident polymorphic file virus.
Affects	COM and EXE files.
File Growth	Variable 4Kb to 5Kb.
Removal	Method 3.
Description	The virus infects files on execution, generating an increase in file size of between 4 and 5Kb. The following string appears in the virus: `Satan Bug virus - Little Loc` This virus targets two anti-virus programs: McAfee Scan and Central Point Anti-Virus. The true identity of the virus author, who also wrote ***Natas***, is known to the authorities.

Saturday 14th (Durban)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, plus one other COM or EXE file chosen at random from the current subdirectory. Date/time are not preserved.
File Growth	670 to 685 bytes.
Removal	Method 1.
Description	This virus uses one of the interrupts that Novell uses, so cannot run on a Novell network. Every Saturday 14th, 100 sectors of rubbish are written to the first sectors of drives D:, C:, B: and A: in that order. This overwrites the boot sector, the FAT and the root directory on most disks. On larger disks it might only overwrite the boot and the FAT. This has some resemblance to ***Jerusalem*** and demonstrates that it isn't wise to set the system clock forward on Friday 13th. The virus handles memory management for itself, and so will escape memory map programs and monitors designed to notice programs going TSR.

Scotts Valley (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	COM: 2,131 bytes; EXE: 2,126 to 2,141 bytes.
Removal	Method 2.
Description	The virus is encrypted. Every Friday during 1991 and thereafter, when files are closed their date/time is set to zero. This is a development of ***Jerusalem***.

Screen+1 (V948)

Type	Memory-resident file virus.
Affects	Program files on execution, and COM and EXE files on opening. COM files larger than 64,256 bytes and EXE files larger than 256Kb are not infected. COMMAND.COM is avoided.
File Growth	948 bytes after rounding up to a multiple of 16 bytes.
Removal	Method 1.
Description	The virus contains the text **command** (in lower case). The virus picks a random position on colour screens, and if the character there is in the range 40h to AFh (@ to ») or E0h to EFh (α to ∩) it changes it to the next character in the character set. It repeats this for as long as it is in memory.

Sector Zero (None)

Type	Trojan.
Affects	N/A
File Growth	N/A
Removal	Delete it using the DOS **DEL** command.
Description	When it is run, it writes garbage to six sectors (starting at 2) of physical device 0 (drive A:) and 3 (which is not likely to be present).

Sentinel (None)

Type	Distributed in Turbo Pascal source code, so must be compiled to spread. Also distributed in compiled form.
Affects	COM and EXE files.
File Growth	Various; around 5Kb.
Removal	Method 2.
Description	The message `You won't hear me but you'll feel me... (c) 1990 by Sentinel. With thanks to Borland` can be found at the end of the virus, and is sometimes displayed. Files are renamed.
Variants	***1, 2, 3, 4, 5***

Shadowbyte (None)

Type	File virus.
Affects	COM files on execution of an infected file.
File Growth	635 or 723 bytes.
Removal	Method 1.
Description	The virus contains `Shadowbyte Lives` backwards. In July, if an infected program is run the computer sounds a rising tone and hangs. The virus attempts to format track 0 of the hard and floppy drives, but a bug prevents this happening. The message should then be displayed, but a bug prevents this too.
Variants	Two different sizes: 635 and 723 bytes.

Shake (None)

Type	Memory-resident file virus.
Affects	The next uninfected COM file in the current subdirectory when any program calls interrupt 21h function 36h (get drive information). Files larger than 60Kb are avoided. Date/time is preserved. Attempts to write to write-protected media are not reported as errors.
File Growth	476 bytes. This is concealed if the virus is in memory.
Removal	Method 1.
Description	There is a 1 in 16 chance that instead of running the program, the computer will beep and display the message `Shake well before use !`. After doing this once, it patches itself so that it doesn't do it again until the next time it goes TSR.

SI-492 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. COMMAND.COM is infected first.
File Growth	492 to 507 bytes.
Removal	Method 1.
Description	After 20 seconds and thereafter once an hour, between 0 and 9 random sectors are written to a random place on drive C:. The specimen available is slightly corrupted.

Simulate (None)

Type	File virus.
Affects	An uninfected COM file in the same directory on execution of an infected file.
File Growth	1,250 to 1,300 bytes.
Removal	Method 2.

Description	Each infection is encrypted differently and the decryptor header is variably scrambled.
	
	If the system clock seconds count is at zero when the program runs, one of several messages will be displayed and the computer hangs. The message are stolen from other viruses:
	
	`HA HA HA YOU HAVE A VIRUS`
	
	`FRODO LIVES!`
	
	`Have you ever danced with the Devil in the pale moonlight?`
	
	`DATACRIME VIRUS RELEASED: 1 MARCH 1989`
	
	`ALIVE... Your system is infected by the SIMULATION virus.. Have a nice day!`
	
	These are encrypted in the virus.
	
	There is a lot of disk activity once all the COM files on a disk have been infected, as each is examined in turn as the virus looks for a file to infect. There is a 1 in 60 chance of a misleading message being displayed and the computer hanging.

SMEG.Pathogen (Pathogen, SMEG v0.1)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution of an infected file, or on access via DOS function 6Ch: Extended Open/Create. COMMAND.COM and some anti-virus programs are avoided. It does not infect files shorter than 32 bytes, COM files longer than 56,000 bytes, or EXE files longer than 512,000 bytes.
File Growth	Variable 4,004 to 4,804 bytes.
Removal	Method 2.

Description	This virus is variably encrypted and highly polymorphic.
	
	Whenever an infected program is executed and the virus installs itself into memory, an internal generation counter is incremented. Thus all files infected incerement the counter by one. When the counter reaches 32 it is zeroed (restarted) and the virus triggers.
	
	When any executable file (i.e. COM or EXE) is being run or accessed via the DOS Extended Open/Create function call, the 32nd generation virus will patch CMOS to disable floppy disk drives.
	
	In addition, if the current day is a Monday and the time is between 5pm and 6pm, the virus displays the message:
	
	`Your hard-disk is being corrupted, courtesy of PATHOGEN!`
	`Programmed in the U.K. (Yes, NOT Bulgaria!) [C] the Black Baron 1993-4.`
	`Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator!`
	`'Smoke me a kipper, I'll be back for breakfast.....'`
	`Unfortunately some of your data won't!!!!!`
	
	Then the virus disables the keyboard and trashes the first 256 cylinders of the hard disk.

SMEG.Queeg (Queeg, Pathogen, SMEG v0.2)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution of an infected file, or on access via DOS function 6Ch: Extended Open/Create. COMMAND.COM and some anti-virus programs are avoided. It does not infect files shorter than 32 bytes, COM files longer tan 54,232 bytes, or EXE files longer than 512,000 bytes.
File Growth	Variable 4,300 to 6,100 bytes.
Removal	Method 2.

Description	This virus is variably encrypted and highly polymorphic.
	
	Whenever an infected program is executed and the virus installs itself into memory, an internal generation counter is incremented. Thus all files infected increment the counter by one. When the counter reaches 32 it is zeroed (restarted) and the virus triggers.
	
	When any executable file (i.e. COM or EXE) is being run or accessed via the DOS Extended Open/Create function call on Sunday between noon and 1pm, the 32nd generation virus triggers with the probability of 1/32nd.
	
	The virus displays the message:
	
	`-» QUEEG «-`
	`~~~~~`
	`(C) The Black Baron 1994`
	
	`Featuring: SMEG v0.2`
	
	`Better than life.....`
	
	Then the virus trashes the first 256 cylinders of the hard disk.

Spanz (None)

Type	File virus.
Affects	A COM file of less than 63,489 bytes on execution of an infected program.
File Growth	639 bytes.
Removal	Method 1.
Description	The virus contains the text `INFECTED! * SPANZ *` at the end. Six months after a file has been infected, if the seconds on the system clock are at 0, it will rename files to INFECTED!. This is a version of ***Vienna***.

Sparse (None)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	3,840 bytes.
Removal	Method 1.
Description	There is no payload. The virus is mostly padding bytes.

Squeaker (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except those with names matching SCAN* OR ??VU*.
File Growth	1,091 bytes.
Removal	Method 1.
Description	Some time after the virus goes TSR the computer makes a 'skreek' noise.

Stack (None)

Type	Trojan.
Affects	N/A
File Growth	N/A
Removal	Delete it using the DOS **DEL** command.
Description	The code contains the text `Infect file` near the end. Whenever a program is run, the message is displayed before the program runs, then it trashes the hard disk.

Staf (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	2,083 bytes.
Removal	Method 1.

Description	This is clearly a demo virus. Each time an infected program is run it displays:
	
	`This program has been infected by:`
	`Virus Demo Ver.:`
	`1.1 - Handles with care!`
	`By STAF (Tel:`
	`(819) 595-0787)`
	`Generation #xx`
	
	where xx is the generation number. There are various other messages in the virus.

Stardot-600 (None)

Type	File virus.
Affects	An EXE file (in a random subdirectory) on execution of an infected program.
File Growth	600 to 615 bytes.
Removal	Method 1.
Description	The last two bytes of the file are '*.', hence the name. Each time an infected program is run there is a one in seven chance that the payload will trigger. When it does, it overwrites 8 sectors of the disk. These are chosen at random in the range 0 to 255 for drives A: and B:, and 0 to 65,535 for C: and above.

Stardot-789 (805)

Type	File virus.
Affects	COM and EXE files when an infected program is run.
File Growth	789 to 805 bytes.
Removal	Method 1.
Description	On September 24th after 7am, the virus overwrites the first 200 sectors of every DOS volume.
Variants	There is a version which does the same thing on February 13th after 1pm. This version adds 817 bytes to files.

Stoned (New Zealand; Marijuana; Australian; Hawaii; Hemp; Sanded; San Diego; Smithsonian; Zapper; Sex Revolution)

Type	Boot and partition sector virus.
Affects	Floppy and hard disks when the computer is booted from an infected (not necessarily a bootable) diskette. The virus copies itself to the hard disk partition sector; any write-enabled diskette accessed in drive A: is infected.
File Growth	N/A
Removal	Method 3.
Description	There is one chance in eight that each time a computer is booted from an infected disk that the message `Your PC is now Stoned` will be displayed. This can be found in the boot sector of infected diskettes and the partition sector of hard disks, together with `Legalise Marijuana`. The boot sector of diskettes is moved to (0,1,3). On 360Kb diskettes this is the last directory sector, which the author believed to be safe. However, on higher capacity diskettes the original boot sector overwrites part of the directory. On a small number of hard disks the original partition sector will overwrite part of the FAT (0,0,7).
Variants	There are a number of variants, as it is easy to patch the message. **Zapper** Using the system clock as a randomiser, 1 infection in 256 triggers the payload. This overwrites the first 16 tracks of the disk followed by the message `I ZAPPED YOU!`. **Sanded:** The message reads `Your PC is now sanded`. **Swedish Disaster:** the message reads `The Swedish Disaster 1`. **Sex Revolution 1.1 and 2:** The message reads `Export of Sex Revolution ver 1.1 (or ver.2.0)`.

cont...

Rostov:
When this infects a diskette it overwrites 8 sectors starting at (8,0,0). On the next infection it does the same on cylinder 9, and so on. Some Western Digital controller cards write data to the partition sector; this will overwrite the original virus message on an infected hard disk and be transferred when the virus replicates.

Stoned-8:
When this infects a hard disk the original partition sector is copied to (0,0,8) and the partition code is replaced. On floppies, the original boot sector is copied to (0,0,5). If the PC is in graphics modes there is a 1 in 16 chance of a message in a non-Roman language being displayed. This is like ***Stoned***, but must not be removed by hand using exactly the same method or the hard disk will not be accessible.

Stoned-16:
When this infects a hard disk the original partition sector is copied to (0,0,16) and the partition code is replaced. On floppies, the original boot sector is copied to (0,1,3). On floppies larger than 360Kb the original boot sector overwrites part of the directory.

Damien:
This is almost identical to ***Swedish Disaster***. It contains the text `Damien Virus (Beta-Test Release 0.1) Written by Metal Thunder 1991 (c) IVRL (Head quarter - Milan Italy).`

Laodung:
When this infects a hard disk the original partition sector is copied to (0,0,8) and the partition code is replaced. If the virus is in memory, diskettes seem to be empty. There is a 1 in 128 chance that it will play a tune.

Noint:
This is based on ***Stoned*** but with major differences. The partition sector is stealthed, so it will appear normal when read.

Other variants: ***Teraz, b, c, d, e, Sonus, Nulls, Donald, Flushed, In love, stoned-floppy, Mexican, WD1*** to ***WD7***.

Stoned dropper (None)

Type	This is not a virus but a virus-dropper. It does no replicate. It purports to be a program which formats floppy disks, but it also installs a copy of ***Stoned*** on the boot sector of each diskette.
Affects	Floppy disks.
File Growth	N/A
Removal	Delete the file, and deal with ***Stoned***.
Description	***Stoned*** is installed. The example examined was called CFORMAT.COM.

Striker (None)

Type	File virus.
Affects	COM files on execution of an infected file.
File Growth	461 bytes.
Removal	Method 1.
Description	The text `Striker #1` can be found near the start of the file.

STSV (V200)

Type	File virus.
Affects	All COM files in the current subdirectory of drive C: (regardless of the current drive) on execution of an infected file.
File Growth	200 bytes.
Removal	Method 1.
Description	The virus contains the text `STSV`.

Stupid (Do nothing)

Type	File virus.
Affects	The first COM file in the current subdirectory when an infected file is run. Date/time and read/write attributes are not preserved.
File Growth	583 bytes.
Removal	Method 1.
Description	There is no self-recognition code, so files can be re-infected. Eventually, running an infected file will crash the system.

Suomi (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	1,008 to 1,023 bytes.
Removal	Method 2.
Description	The virus is encrypted. When a file has been infected for 17 days, it disinfects that file, disables the keyboard, writes rubbish to the screen and hangs the computer.

Superhacker (Murphy; Talentless Jerk; Harare)

Type	File virus.
Affects	A COM or EXE file on execution of an infected file. Only files between 9 and 61,440 bytes are affected.
File Growth	1,077 bytes.
Removal	Method 1.
Description	The file contains `Murphy`, but the message is encrypted. If the date is a multiple of 4 and the seconds are a multiple of 4, the virus displays `Craig Murphy calls himself SUPERHACKER but hes just a talentless jerk!`. It creates a file called ^^^^^^^^ in the root directory, then deletes it. EXE files are disinfected when they are run. This is completely unrelated to ***Murphy-1*** and ***Murphy-2***.

SVC (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. Only files between 1,024 and 63,811 bytes are affected.
File Growth	Version 4: 1,689 bytes. This is concealed from **DIR** if the virus is in memory.
Removal	Method 1.
Description	The text `(c) 1990 by SVC,Vers 4.0` can be found at the end of the virus.
Variants	**SVC 3.1:** Files grow by 1,064 bytes. COM files smaller than 1Kb, or of 25,312 or 25,307 bytes, possibly to avoid infecting some versions of COMMAND.COM. It also avoids infecting programs with **AI** or **SC** in the name. This is probably to avoid infecting AIDSOUT (a Russian anti-virus program) and SCAN. The virus contains the text `(c) 1990 by SVC,Vers. 3.1`. **SVC 5.0:** Files grow by 3,103 bytes. The virus is fully stealthed. **SVC 6.0:** Files grow by 4,644 bytes. The virus is fully stealthed – it also infects partitions, so Method 3 should also be used.

SVIR (None)

Type	File virus.
Affects	The next EXE file in the current subdirectory on execution of an infected file. Attributes and date/time are not preserved.
File Growth	512 to 527 bytes.
Removal	Method 1.
Description	After using the file for a while there will be a large number of unrequested accesses to drive A:. The virus contains a counter which starts at 55, and each time an infected program is run the counter is decremented. When it reaches zero it tries to access drive A: each time the infected program is run. If there is no disk in the drive the normal error message will be displayed.

Swami (Bhaktivedanta)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, except those matching *ND.COM (so COMMAND.COM is not infected). COM files between 1,250 and 64,000 bytes and EXE files between 1,250 bytes and 64Kb are affected.
File Growth	1,250 bytes.
Removal	Method 1.
Description	The text string `Bhaktivedanta Swami Prabhupada (1896-1877)` can be found in the virus. If a file matching the name ***AN.EXE, *LD.EXE** or ***RJ.EXE** is run, the virus attempts to reboot the computer with an interrupt 19h; on some machines this reboots but on others it hangs the system. On Saturdays, if a COM file is run the first EXE file in the directory is deleted. Every April 15th an EXE file is deleted each time a program is run. The virus uses part of the ***Dark Avenger*** code to access the firmware for writing to the disk instead of going via interrupt 13h.

Swiss-143 (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	143 bytes.
Removal	Method 1.
Description	No payload.

Sylvia (Holland Girl; Holland)

Type	File virus.
Affects	Four uninfected COM files on execution of an infected program. COMMAND.COM, IBMBIO.COM and IBMDOS.COM are avoided, presumably to avoid detection. Attributes are preserved. This is one of the few viruses that infects by making an infected copy and deleting the original.
File Growth	1,332 bytes.
Removal	Method 1.

Description	When an infected file is run there is a lot of disk activity as the virus looks for a file to infect.
	
	The message `This program is infected by a HARMLESS text-Virus V2.1 Send a FUNNY postcard to : Sylvia Verkade, 1 Duinzoom 36b, 3235 CD Rockanje The Netherlands. You might get an ANTIVIRUS program.....` Is in the virus but not displayed.
	
	The virus checksums this message each time it runs, and if it has been altered it displays:
	
	`FUCK YOU LAMER!!!!`
	
	`system halted...`
	
	and the system hangs.

Variants	**Kranz:** The text at the beginning has been altered to `This program is infected by a ******** KranzVirus *12*` and the address has been changed. Because the checksum hasn't been patched, the computer hangs when it is run. The message which should be displayed has been patched using asterisks. Since running this virus hangs the computer, it cannot spread. **Hong Kong:** Also doesn't work. It contains a political message. **Minor variants:** *a, b, c, d*

Syslock (Macho; 3551; Macrosoft)

Type	File virus.
Affects	A COM or EXE file (chosen randomly from the current drive) on execution of an infected file. The virus is encrypted and decrypts itself at run time. The virus looks for a DOS subdirectory off the root, and if it finds one creates a hidden system file called KEYB.PCM.
File Growth	3,551 to 3,566 bytes.
Removal	Method 2.
Description	If the environment contains SYSLOCK=@ the virus does nothing – it doesn't even infect files. Otherwise, it works its way down the disk 32 sectors at a time, converting each occurrence of the word Microsoft to Macrosoft (or Machosoft in the ***Macho*** version). It uses KEYB.PCM to mark the point it has reached in making the changes. If there is no subdirectory off the root called DOS is doesn't create the KEYB.PCM file and so doesn't make the changes.
Variants	**Cookie (Cookie-2232):** Files grow by padding to a multiple of 16 bytes then adding 2,232. If the year is 1988 or later and the date is April 1st or later, running an infected program sometimes triggers the trick. The screen clears and `I want a Cookie!` Is displayed in the centre. If you type `Cookie` the original program will run. **Xmas:** This is a variant that displays a growing number of candles on the days up to Christmas.

Taiwan-708 (None)

Type	File virus.
Affects	An uninfected COM file on execution of an infected file. The DOS write-protect error message is suppressed. Date/time and read/write attributes are preserved except that the seconds field is set to 62.
File Growth	708 bytes, or to 1,416 if they are less than 708 bytes.
Removal	Method 1. If the payload triggers you will need to reformat the hard disk and restore backups.
Description	Program loading is slowed by the search for uninfected files. On the 8th, garbage is written to the first 320 sectors of the current drive and drive D:, starting at the boot sector and overwriting both FAT copies and the root directory. The message `Greetings from the National Central University! Is today sunny?` Is then displayed.
variants	**Taiwan-743:** Files grow by 743 bytes unless they are smaller, in which case they grow to 1,486 bytes. Only 160 sectors are overwritten, and after the message it waits for a keypress.

Telefonica-boot (Kampana-boot)

Type	Memory-resident boot and partition sector virus.
Affects	Hard and floppy disks when the computer is booted from an infected (not necessarily bootable) floppy disk. If the computer is booted from an infected hard disk the virus goes TSR and infects any diskette in drive A:.
File Growth	N/A
Removal	Method 3.
Description	The text `Campana Anti-TELEFONICA (Barcelona)` is encrypted in the virus. **Hard disks:** the original partition is copied to (0,0,7). The virus uses stealth techniques: if you examine (0,0,1) the original partition record is displayed, and if you look at (0,0,6) or (0,0,7) you are shown (0,0,5). This conceals the rest of the virus. **Floppy disks:** the original boot sector is copied to (0,1,3). After 400 boots the Trojan triggers. This overwrites the hard disk with garbage and then displays the message.

Tenbytes (1554; Usenet; 1559; 9800:0000; Valert; Tenbytes-1554)

Type	Memory-resident file virus.
Affects	COM (over 1,000 bytes) and EXE (over 1,024 bytes) files on execution. Read/write attributes are preserved.
File Growth	COM: 1,554 to 1,569 bytes. EXE: 1,514 to 1,529 bytes.
Removal	Method 1.
Description	Between September and December, whenever DOS writes to a file the first 10 bytes are omitted and 10 bytes of garbage are added at the end. Program and data files are affected. The memory-resident part of this virus is in memory that has not been reserved. This makes it vulnerable to being overwritten, but it will be undetectable by memory map programs.

Tequila (None)

Type	Memory-resident file and partition sector virus.
Affects	The partition sector when an infected file is run. When the computer is booted the virus goes TSR and infects every EXE file run.
File Growth	2,468 bytes, but this is stealthed if the virus is in memory.
Removal	Method 1, then Method 3.

Description	The virus is variably encrypted with a self-garbling header. This, with the dual infection mechanism, makes it hard to recognise; it is polymorhpic.
	
	The message:
	
	`Welcome to T.TEQUILA's latest production. Contact T.TEQUILA/P.o.Box 543/6312`
	
	`St'hausen/Switzerland. Loving thoughts to L.I.N.D.A BEER AND TEQUILA FOREVER !`
	
	It will only do this if you put 0FE03h into the AX register and call interrupt 21h, but the virus itself doesn't do it; instead, it displays `Execute: mov ax, FE03 / int 21. Key to go on.`
	
	Exactly three months after the virus is installed on the hard disk, and each month thereafter on the date that is an exact number of months after installation, the virus pops up a colourful block graphic display when an infected program is run.

Terror (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution or opening. COM files must be between 1Kb and 64,000 bytes.
File Growth	1,085 to 1,100 bytes.
Removal	Method 1.
Description	The virus contains `Terror` at the end.

Testvirus B V1.4 (None)

Type	File virus.
Affects	All COM files in the current subdirectory on execution of an infected file, but only if you choose the 'infect' option.
File Growth	1,000 bytes.
Removal	Method 1.

Description	Files contain `This is TESTVIRUS B V1.4` near the beginning. This is displayed each time the program runs. It then gives the options:
	
	`1 = infect .COM files of this directory and run the original program`
	
	`5 = run only original program`
	
	`9 = abort`

Thanksgiving (V1253)

Type	Memory-resident file, boot and partition sector virus.
Affects	COM files on execution, and floppy and hard disks on access. Date/time and read/write attributes are not preserved, and the **Abort, Retry, Ignore?** message is not suppressed if a floppy is write-protected.
File Growth	1,253 bytes.
Removal	Method 1, then Method 3.
Description	**Floppy disks:** the boot sector is replaced and moved further up the disk. **Hard disks:** the partition sector is replaced and moved further up the disk. When the virus is installed by booting from an infected disk, 64Kb of memory is no longer available. On the 23rd November 1990 and thereafter the payload is triggered. This overwrites 17 sectors on heads 0 and 1 of the hard disk, stepping through the cylinders from 0. There is no stopping point, so the virus will go as far as cylinder 255 then cycle back to 0 and continue. The hard disk will then be unreadable. 22nd November 1990 was Thanksgiving Day in the USA.

The Rat (None)

Type	Memory-resident file virus.
Affects	EXE files on execution or opening.
File Growth	None. Overwrites 384 bytes of the header starting at offset 128.
Removal	Method 1.
Description	The virus contains `The Rat, Sofia` at the end. There is also a message in Bulgarian inside, which is not displayed. There is no payload.

Thirteen minutes (V711)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files over 1,700 bytes are affected; COMMAND.COM is avoided.
File Growth	704 bytes plus a random number in the range 0 to 15.
Removal	Method 1.
Description	Thirteen minutes after infection there is a 25% chance of each diskette failing to write and giving a timeout error code.

Thursday-12th (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, opening or creation. It avoids COMMAND.COM and any files starting with SCAN, CLEAN, VIR, ARJ and FLU.
File Growth	2,161 to 2,176 bytes.
Removal	Method 1.
Description	The virus contains the encrypted text `VirCheck V1.2 (C)1991 Be aware of those worms out there, violating your machine on Friday 13th - it's tomorrow!`, but this is not displayed.

Tiny (None)

Type	Memory-resident file virus.
Affects	The first uninfected write-enabled COM file in the current subdirectory on execution of an infected file.
File Growth	Varies depending on the version: 133, 134, 138, 143, 154, 156, 158, 159, 160, 167, 198.
Removal	Method 1.
Description	There is no payload. This is not related to ***Tiny*** which grows files by 163 bytes.
Variants	About a dozen, with sizes as listed above.

Tiny (None)

Type	File virus.
Affects	Uninfected COM files in the current subdirectory on execution of an infected file. The floppy disk write-protect error message is not suppressed.
File Growth	163 bytes.
Removal	Method 1.
Description	There is no payload.

Tiny-127 (None)

Type	File virus.
Affects	A COM file in the current subdirectory on execution of an infected file. Date/time is not preserved.
File Growth	127 bytes.
Removal	Method 1.
Description	There is no payload.
Variants	**Tiny-123:** Files grow by 123 bytes. **Tiny-Mutant:** Files grow by 127 plus the generation count.

Tiny-128 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. The virus overwrites the upper end of the interrupt vector table. Date/time is not preserved.
File Growth	128 bytes.
Removal	Method 1.
Description	There is no payload.

Traceback (3066)

Type	Memory-resident file virus / file virus.
Affects	There are two mechanisms: 1. Memory-resident, infecting COM and EXE files on execution. 2. Direct (after December 1988) infecting a COM or EXE file on execution of an infected program. The resident portion occupies 7Kb of memory.
File Growth	3,029 to 3,066 bytes.
Removal	Method 1.
Description	An hour after the virus goes TSR a falling letters display is triggered. This is different from ***Cascade*** in that the display is silent and the characters fall in a different way. They can be made to rise up again by pressing keys until they are all at the top of the screen. There is no major damage.
Variants	**Spanish (Traceback-2930):** An earlier version. Files grow by 2,930 bytes.

Trackswap (Xswap; XBoot)

Type	Memory-resident boot sector virus.
Affects	Floppy disks when the computer is booted from an infected (not necessarily bootable) floppy.
File Growth	N/A
Removal	Method 3.
Description	Some diskettes may be corrupted. **360Kb diskettes:** the boot sector is copied to (0,1,3) which is the seventh directory sector and is rarely in use. **1.2Mb diskettes:** the boot sector is copied to (0,1,3) which is the third directory sector. If this is in use the directory listing starts OK but becomes gibberish after a few dozen lines.

Trash (None)

Type	Not a virus.
Affects	N/A
File Growth	N/A
Removal	Delete the file. If the partition has been zeroed, run **CleanPart**, or format the drive and restore from backups.

Description	The program displays the message:
	
	`********** W A R N I N G ! ! ! **********`
	`This program, when run, will zero (DESTROY!) The master boot record of your first hard disk.`
	
	It then explains that its purpose is to test anti-virus software. You have to press Ctrl Alt to proceed, a combination which would be very hard to press accidentally.
	
	This demonstrates that a hard disk can be trashed even though a protection program is installed. It does so successfully.

Tremor (None)

Type	Memory-resident file virus.
Affects	Fast infector: COM and EXE files on execution and almost any access. COM files are infected only if they start with 0E9h (JMP instruction).
File Growth	4,000 bytes
Removal	Method 1.

Description	This virus is variably encrypted and highly polymorhpic.
	
	When an infected file is executed, the virus stays memory-resident, possibly in UMB or Extended Memory (if available), and infects COMMAND.COM. The virus demonstrates full stealth techniques – if it is memory-resident, no changes to infected files are visible.
	
	Approximately three months after infecting the computer the virus triggers. On every Ctrl Alt Del warm boot the following message is displayed:
	
	`-= T.R.E.M.O.R. was done by NEUROBASHER /May-June'92 Germany =-`
	
	`-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-`
	
	In addition, if more than 255 files were created or opened (e.g. via the COPY command) since the last system reboot, the virus starts to salute every DOS call with a random sound and screen display tremor.

Trivial (None)

Type	Overwriting file virus.
Affects	First COM file in the current subdirectory.
File Growth	None.
Removal	Method 2.
Description	The virus is only 30 bytes long. Both program and data files are overwritten.
Variants	There are a number of versions and rewrites of this, with lengths between 25 and 200 bytes. All of them are overwriting viruses and cannot be a genuine threat.

Tumen (None)

Type	Memory-resident file virus.
Affects	A COM file on execution of an infected file. Files over 64,885 bytes are not infected. Date/time and attributes are not preserved.
File Growth	1,092 to 1,663 bytes, depending on variant.
Removal	Method 1.
Description	***Tumen.1663*** contains **`Full moon tonight... The time of Wolfbacks... U...U...U... This is only demonstration version, but you hear some howl.`** Near the end is: `(C) Copyright MMA Company All rights reserved. USSR Tumen 1990-v0.5 This program was created in Tumen by group three Wolfbacks at April,1990 General System_&_Files affecting effects by Max Main consultant -Tall Lazy Micle General Music_&_Video harmless effects by Alex BACKWOLFS OF THE WORLD, UNITE ! ! !` If you press Ctrl Alt and any key, a tune is triggered and palette effects are displayed on EGA and VGA monitors. Every time a file is infected the palette effect is triggered.

cont...

Variants	**Tumen.1092:** This is very different but somewhat related. Files grow by 1,092 bytes and the virus contains the text `Be carefull... Hackers time tonight... This present was created in Tumen at 1990. v.2.0.(c) Max Soft corporation` and `Hackers of the world, Unite !`. There is a counter (set at 51 in the specimen received) which is incremented each time a file is infected. When the counter reaches 112 the Trojan triggers, which overwrites cylinders 0 to 255, head 0, sectors 1 to 16. Before the Trojan triggers, each time an infected file is run the virus reads the boot sector and writes it back unchanged. Presumably this is to acclimatise the user to any interrupt blocker giving regular false alarms. While the virus is memory-resident, files cannot be deleted or renamed; possibly this is a defence against anti-virus products. Files larger than 64,000 bytes are not infected. Two other variants are ***Tumen.1255*** and ***Tumen.1242***.

TUQ (RVPS)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	453 bytes.
Removal	Method 1.
Description	The virus contains the text `VIRUS`. It has no payload.

Twelve Tricks (None)

Type	Trojan.
Affects	Leaves part of itself on every affected hard disk.
File Growth	N/A
Removal	Method 3.
Description	This is a program run by the user. As well as the obvious things, it lays down a new partition sector. The new partition sector contains the text `SOFTLoK V3.0 SOFTGUARD SYSTEMS INC 2840 St. Thomas Expwy, suite 201 Santa Clara, CA 95051 (408)970-9420.` **It should be pointed out that there is no evidence that the company mentioned has anything whatsoever to do with the Trojan; perhaps the author has a grudge against them.** When the Master Boot Record is run, which is every time the computer is booted from the hard disk, the Trojan installs itself. A random number generator determines which of the tricks will be installed. The twelve tricks are: 1. Insert a random delay loop in the timer tick. This slows down the machine and it runs rather jerkily. 2. Insert and End-Of-Interrupt in the timer tick. This interferes with the servicing of hardware interrupts so that, for example, the clock is stopped or TSRs which depend on the timer tick don't work, or the floppy drive motor is permanently on. 3. Every time a key is pressed or released, the timer tick count is incremented by a random number. This has a variety of effects: programs sometimes won't run; when you type 'TIME' you get **Current time is divide overflow**; copying files sometimes doesn't work. 4. Every time interrupt 0Dh is executed the routine is only completed three times out of four. This interrupt is used on PCs and XTs for the fixed disk, and on ATs for the parallel port.

cont...

	5. Every time interrupt 0Eh is executed, the routine is complete only three times out of four. This interrupt is used for the floppy disk. 6. Every time interrupt 10h is called (the video routine), insert a random delay loop. This slows down the screen and makes it run jerkily and/or slowly. 7. Every time the video scroll up routine is called, instead of scrolling the requested number of lines the entire scrolling window is blanked. 8. Every time a request is made to the floppy disk handler it is converted to a write request. Thus the first time you try to read from or write to a diskette, whatever happens to be in the buffer will be written and will probably overwrite the boot sector, FAT or directory, as these must be read before anything else can be done. If you try to read a write-protected diskette, the write-protect error message is displayed. If you do a DIR of a write-enabled diskette the **General failure...** message is displayed, and if the diskette is inspected using a sector editor, the boot and FAT will have been zeroed or overwritten. 9. Every time interrupt 16h is called (read the keyboard) the flags for Caps Lock, NumLock, Shift etc. are set randomly before the keystroke is returned. This means that the keyboard will only work occasionally at the DOS prompt, and programs which poll interrupt 16h will be unusable. Holding down the Del key will trigger a warm reboot.

cont...

10. Everything that goes to the printer is garbled by XORing it with a byte from the timer tick count, which is in effect a random number.
11. Every character sent to the printer has its case reversed by XORing it with 20h. Non-alpha characters are XORed so that a space becomes a null and line feeds don't feed lines.
12. Whenever the Time-Of-Day interrupt (1Ah) is executed, and End-Of-Interrupt is executed instead. These means that the system clock cannot be set and the time is set permanently to one value.

There are two more things the Trojan does: it uses a random number generator to trigger a low-level format of the track containing the active boot sector one time out of 4,096, which will also destroy part of the first copy of the FAT. After this, it displays the message and hangs the computer. If it doesn't do the format, it makes a random change to a random word in one of the first 16 sectors of the FAT, which will cause a slight and increasing corruption in the file system. This is perhaps the worst thing it does, as it will cause an increasing corruption of the files on the disk.

The program that drops the Trojan was, in the specimen analysed, a hacked version of CORETEST, which is a program to benchmark hard disk performance. Although this is not a virus, it is unlikely that all the patching to the original program was done by hand; it is far more likely that the author wrote a prepender program to automatically attach his code to the target executable file. If this is the case, there are two consequences: the first is that he might have Trojanised other programs; in other words, there may well be other droppers around. The second is that, if this is the case, the encryption cannot be relied upon to have the same seed each time, as the prepender could change the seed each time it operates. So it would be unsafe to search files for the encrypted Master Boot Record.

Indeed, a further possibility exists, in that the prepender program might have been placed into circulation and people running it could unwittingly be creating additional droppers. There is absolutely no evidence to suggest that this is actually the case, but anyone who detects this dropper in one of their files should take great care to examine all the others.

Twin (None)

Type	Memory-resident file virus.
Affects	Every time an EXE file is run, a hidden COM file with the same name is created. When the program name is typed, the COM file is run instead of the EXE file, making the virus memory-resident. The virus then runs the EXE file.
File Growth	None.
Removal	Power off and boot from a clean DOS diskette. Delete all the hidden COM files, which are 351 bytes long. Alternatively, use `FINDVIRU /REPAIR /DELETE`.
Description	If the virus is in memory, DOS doesn't report the hidden files.

Uruguay.6 (Uruguvau)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution, opening or creation of an infected file. Files shorter than 57,344 bytes are not infected. COMMAND.COM and some anti-virus programs are avoided.
File Growth	4,879 bytes.
Removal	Method 1.

Description	This variably encrupted and extremely polymorphic virus is able to survive a warm boot (Ctrl Alt Del). It is a semi-stealth virus: the growth of infected files is concealed and the virus is memory-resident.
	
	If an infected file is executed when the virus is already memory-resident, there is a probability of 1/256 that the virus triggers and displays this message followed by a random tune:
	
	`'Uruguay-#6' Virus`
	`programmed in Montevideo (URUGUAY) by F3161. 11/92`
	`This is a research virus - DO NOT DISTRIBUTE.`
	
	The virus can also trigger on a warm reboot.

Variants	There are currently eight variants known – ***Uruguay.1*** to ***Uruguay.8***. They differ in their levels of polymorphism, infected file growth and displayed messages. Earlier versions are less polymorphic and cannot survive a warm boot.

USSR-707 (V707)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files smaller than 61,440 bytes are affected. This only works on DOS 3.3 systems.
File Growth	707 bytes.
Removal	Method 1.
Description	There is no payload.

V2P6 (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	1,900 to 2,400 bytes.
Removal	Method 2.
Description	This virus is so polymorphic that there is not even a consistent sequence of two bytes for signature scanners to identify. This is in the same family as ***Chameleon***.

V-Sign (Cansu)

Type	Memory-resident boot and partition sector virus.
Affects	Floppy and hard disks.
File Growth	N/A
Removal	Method 3.
Description	This virus infects hard and floppy disks of read and write access (e.g. DIR command). ***V-Sign*** is slightly polymorphic: it changes the order of some instructions on every infection, resulting in six slightly different 'incarnations'. The virus can detect disks infected with ***Stoned***, which it removes and then reinfects the disk with itself. If the virus succeeds in infecting 64 disks since the last system boot, it triggers. A big V-sign is displayed on the screen and the computer hangs.

Vbasic (None)

Type	File virus.
Affects	Four COM or EXE files (starting in the current directory) on execution of an infected file. EXE files are infected before COM files. BASRUN.EXE, BRUN.EXE, IBMBIO.COM. IBMDOS.COM and COMMAND.COM are ignored. Date/time and read/write attributes are preserved.
File Growth	5,120 to 5,135 bytes.
Removal	Method 1.
Description	COM files are not infected correctly and don't work. When an infected file is run there is a lot of disk activity as the virus looks for files to infect. After April 1st 1992, when an infected program is run it infects all other programs on the disk and displays the **Access denied** message on the screen. This virus looks as if it has been written in a higher level language than assembler, due to the way each subroutine is called.
Variants	**Vbasic.B:** File growth is 5,120 bytes, but the filenames used are different: KEYB*.COM, KEYB*.EXE, BRUN, BASRUN, COBRUN and NET$OS. **Vbasic.C:** As ***Vbasic.B***, but the filenames used are BRUN, BASRUN, COBRUN, NET$OS, LOGIN, USERLIB and AV.

Vcomm (Polish; 637; Vcomm.A)

Type	Memory-resident file virus.
Affects	An uninfected EXE file in the current subdirectory on execution of an infected file. While infecting it renames the file with no extension so that if the system hangs in the middle of infection the user isn't left with a partly infected file. Read/write attributes are preserved. Critical error handling is not disabled, so attempts to infect files on write-protected diskettes are reported as errors.
File Growth	637 to 1,148 bytes.
Removal	Method 1.
Description	The virus installs a small routine which converts all disk writes to reads. Thus, as long as it's in memory the user can't create, copy, change or delete a file. On monochrome systems the first disk access will hang the system. CGA monitors show a slight snow effect.

VDV-853 (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	853 bytes.
Removal	Method 1.
Description	The messages are encrypted in the virus so can't be seen. Between December 24th and 26th, when an infected file is run it displays a Christmas tree in block graphics with the message: Frohliche Weihnachten wunscht der Verband Deuscher Virenliebhaber Ach ja, und dann wunschen wir auch noch viel Spass beim Suchen nach den Daten von der Festplatte! gez. VDV,December 1990 The next time a key is pressed, rubbish is displayed on the screen and COMMAND.COM is overwritten with the Christmas tree and message.

VFSI (None)

Type	File virus.
Affects	A COM file in the same directory on execution of an infected file. Read-only files are ignored.
File Growth	445 to 453 bytes.
Removal	Method 1.
Description	Each time an infected program is run there is a 20% chance of the following screen changes: the display changes to 40-character mode, clears, and the message `HELLO!!! HAPPY DAY and SUCCESS` appears in yellow, under it `from virus 1.1 VFSI-Svistov` in blinking red. Then the screen is cleared and the program runs.

Victor (None)

Type	Memory-resident file virus.
Affects	A COM or EXE file on one of several DOS function calls. Files shorter than 2,442 bytes and COM files larger than 62,198 bytes are not infected. Critical error handling is disabled, so attempts to infect a write-protected diskette are not reported. Date/time and read/write attributes are preserved.
File Growth	2,443 to 2,458 bytes, depending on rounding.
Removal	Method 1.
Description	The virus contains the text `Victor V1.0 The Incredible high Performance Virus Enhanced versions available soon. This program was imported from USSR. Thanks to Ivan.` On Wednesdays between 9am and 10am, 11am and 12 noon, 1pm and 2pm, and 3pm and 4pm, files in the current subdirectory are deleted.

Vienna (648; 1-in-8; Austrian; DOS-62; First Austrian; DOS-68; Unesco; Charlie; Vienna-648)

Type	File virus.
Affects	The next uninfected COM file in the current directory or on the path, on execution of an infected file in any directory.
File Growth	648 bytes.
Removal	Method 1.
Description	One in eight infections makes the file unusable by patching code for a reboot at the beginning of the file. Eventually COMMAND.COM is infected, so that whenever the computer is started up it just keeps rebooting. The seconds field of the directory is used to store the impossible value 62.
Variants	The source code for this virus has been published in a book, with slight modifications, so there are a large number of viruses based on it. It is commonest in Austria, where it has been given several names. The patching code in the typed-in variants hang the machine, and they do not search down the path for an uninfected file. The viruses described below are all nearly functionally identical to the original, but there seem to have been attempts to reduce the byte-count. The name refers to the byte count/file growth. **Vienna-71a1:** Only files between 10 and 64,000 bytes are infected. **822:** When an infected program is run the virus checks drive A: and tries to read the track after the last. If it succeeds and finds the bytes 52,2 as the first two, it runs whatever is on the diskette. **Vienna-744 (Grither):** Programs are patched so that when they run they overwrite the first 160 sectors of drive C: and display <>`THE GRITHER` <> `Courtesy of Elexion`.

cont...

733:
Only files between 10 and 64,000 bytes are infected. Most of the virus is encrypted by subtracting 1 from each byte. On the 2nd of the month, each time an infected program is run the virus whistles until the timer chip is reprogrammed.

716:
On an after September 4th 1990 it formats all floppies.

656:
In February 14th, March 14th, and from April to December, drive C: is overwritten from the first FAT sector for 80 sectors.

648:
The far jump at the end is corrupted so that instead of jumping to the reboot location it jumps to a random location. There is also a version where the location is correct.

646:
Files grow by 646 bytes.

646b:
A slight variation of ***646***.

645:
Only files between 10 and 64,000 bytes are infected.

644:
Only files larger than 1,280 bytes are infected. Infection only takes place if the time is less than 20 minutes past the hour. There is no Trojan, and the self-recognition bytes are different but still in the file time-stamp.

627:
This is produced by assembling the disassembly with the Microsoft Assembler, which optimises the code by omitting unnecessary zeroes, reducing the length to 627 bytes. A bug means that the 1-in-8 routine is disabled, so the damage routine is never called.

cont...

	623: A critical error handler has been added so that DOS doesn't give the write-protect error message if a write-protected floppy is accessed. The damage routine is enabled; this may be intended as a low-level format, but it tries to execute the BIOS signature instead and the system hangs. **622:** One in eight files has its first 5 bytes patched so it won't run. **583** As ***622***. **582:** As ***622***. **535:** This has 58 in the timestamp seconds field, and patches one in eight files with 5 random bytes. **528:** The virus contains the text `Warning : File is damaged by virus !!!`. This is displayed every time a file is infected. **510:** This has a major bug preventing it from working. If it did it would be a version of ***Vienna***. **435:** This is smaller because the stack is used for storage instead of local variables. The damage routine performs a low-level format on many hard disk controllers; this is not automatic, as the controller asks a number of questions before it formats.

cont...

	367: As ***435***, but the jump is patched to go to the location used by OMTI controllers for the low-level format routine. There is also a cunning coding trick which allows an area of code to be used in multiple roles, saving bytes. **353:** As ***367***, with a few more optimisations. **348:** As ***353***, with more optimisations. Other variants have the sizes 361, 377, 534, 547, 618, 625, 634, 757, 774, 776.

Vienna-534 (W13.A)

Type	File virus.
Affects	The next uninfected COM file in the current directory on execution of an infected file.
File Growth	534 bytes.
Removal	Method 1.
Description	There is no payload, but infected files are dated the 13th of the month. This is a modification of ***Vienna***.
Variants	**Vienna.W13B:** Files grow by 507 bytes.

Vienna-Iraqui (None)

Type	File virus.
Affects	A COM file on execution of an infected file. Only files between 10 and 64,000 bytes are affected.
File Growth	777 bytes.
Removal	Method 1.
Description	An error means this cannot replicate more than once from the original file. The virus contains the strings `I come to you from The Ayatollah! (c)1990, VirusMasters` and `An Iraqui Warrior is in your computer....` One file in eight has a reboot patched into the start of the file instead of being infected (except that the reboot can't work). When this happens the second message is displayed. This is very like ***Vienna***.

Violator (None)

Type	File virus.
Affects	A COM file on execution of an infected file. Only files between 10 and 64,000 bytes are affected.
File Growth	1,055 bytes.
Removal	Method 1.

Description	The virus contains the text:
	
	`TransMogrifed (TM) 1990 by`
	`RABID Ntnl Development Corp.`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`!Copyright (C) 1990 RABID !`
	`!Activation Date: 08/15/90!`
	`!! - Violator Strain 1 !`
	`!(Field Demo Test VErsion)!`
	`! *NOT TO BE DISTRIBUTED* !`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	
	The payload is triggered on or after August 15th 1990; this does a low-level format of cylinder 0 head 0. The device to be formatted is randomly selected, but the virus then steps through all other devices.
	
	This is another version of ***Vienna***.

Variants	**Violator B3:** Files grow by 843 bytes. After December 25th 1990 the virus tries to format drives C to Z but fails. It also tries to overwrite the first 800 sectors of drive C: with the text `Violator Strain B3 - Rabid Nat'nl Development Corp.`.

Violator-Arf (None)

Type	File virus.
Affects	A COM file on execution of an infected file. Only files between 10 and 64,000 bytes are affected.
File Growth	1,000 bytes.
Removal	Method 1.
Description	The virus contains the text `Arf Arf Got You! - RABID 90.` If the date is later than October 10th 1990 the message is displayed and physical drives 0 to 25 are formatted. This normally means that the A: and B: drives are formatted. This is very like ***Vienna***.
Variants	**Violator-arf.s:** If the year is 1992 or later, the virus displays `If this one escapes, I am fucked up.` When an infected program is run. It then triggers the payload, which formats track 0 head 0 of all floppy drives; it looks as though it was meant to format floppy and hard disks, but contains a bug.

Violator B4 (None)

Type	File virus.
Affects	COM files on execution of an infected file. Only files between 10 and 64,000 bytes are affected.
File Growth	5,302 bytes.
Removal	Method 1.
Description	The virus contains the string `Violator Strain B4 - Written by The RABID Natn'l Development Corp.` and several more lines of text. All interrupt 21h, 13h and 26h calls are done by calling subroutines. This avoids the usual sequence of interrupts seen in most viruses. The intention is to low-level format all drives and overwrite DOS devices with garbage. This doesn't work because of bugs. This is very like ***Vienna***.

Virdem (None)

Type	File virus.
Affects	The next uninfected COM file on drive A: on execution of an infected file. Critical error handling is not disabled, so attempts to infect files on write-protected diskettes are reported as errors.
File Growth	Files smaller than 11KB: 2,559 bytes. Larger files by 792 to 1,616 bytes.
Removal	Method 1. If ***Disktrash*** is triggered, reformat the hard disk and restore from a backup.
Description	When an infected program is run, the user is asked (in German) to guess a number between 0 and n, where n is the generation number of the virus plus 1. If the guess is correct the program runs, else it returns to DOS. This was written as a demonstration virus by Ralf Burger, and distributed as such.
Variants	**Virdem English:** The messages are in English instead of German. **Virdem Disktrash:** This trashes the hard disk if the guess is incorrect. **Virdem.2:** Files grow by 824 bytes. If contains the string `Datum falsch Bitte DATE aufrufen`. If the date is 1980 it displays the message and exits without running the host program. **Virdem-1542:** This is a partially-overwriting virus, but most programs will continue to work after infection. Files grow by 1,542 bytes (or more if the file is smaller than 1,542 bytes). The messages are patched out. There is no payload apart from some programs not working, as the infection overwrites four of the original bytes. *Do not use* **FindVirus** with **/REPAIR;** delete infected files and replace them. Also ***Wonderful, 792.***

Virus-101 (None)

Type	File virus.
Affects	The next COM file on drive A: or B: on execution of an infected file. Date/time and read/write attributes are preserved.
File Growth	2,560 bytes.
Removal	Method 1.

Description	When an infected file is run on the 9th, 18th or 27th the display is triggered. This consists of white bars moving down the screen from the top, followed by a reboot. On any other date the diskette boot sector is patched; if the letters 'No' (as in **Not a system diskette**) appear in the boot sector, everything from there on is replaced by:
	
	`This file has been safely infected by`
	
	`VIRUS101 - the safe, educational virus utility.`
	
	`This copy furnished to John McAfee.`
	
	This message is checksummed and if it is incorrect the program halts; if not, the message is displayed.

Variants	**Virus-90:** An earlier version. Files grow by 857 bytes. When an infected program is run it displays `infected!` before running the program. The virus contains the name and address of the author. Both these viruses were written as a demonstration so that people could safely experiment with them – hence the fact that they only infect drives A: and B:.

Virus-B (Friday 13th; 423)

Type	File virus.
Affects	All uninfected COM files in the current directory on execution of an infected file in any directory. COMMAND.COM is not infected. Date/time and read/write attributes are not preserved. Critical error handling is not disabled, so attempts to infect files on write-protected diskettes are reported as errors.
File Growth	540 to 560 bytes, according to the version.
Removal	Method 1.

Description	Every Friday 13th, infected files are deleted after they are loaded into memory and executed. This does not prevent further infection.
	
	Version 1: When an infected file is run the message:
	
	`WARNING!!!! THIS PROGRAM IS INFECTED WITH VIRUS-B!`
	
	`IT WILL INFECT EVERY ..COM FILE IN THE CURRENT SUBDIRECTORY!`
	
	Is displayed and the computer beeps.
	
	Version 2: COM files grow by 423 bytes, but are not infected.

Virus Construction Set (VCS)

Type	File virus.
Affects	A COM file on execution of an infected file. The virus is encrypted, and if interrupt 26h is located above segment 1000h (for example, if an active monitor is enabled) it doesn't infect.
File Growth	1,077 bytes.
Removal	Method 1.
Description	This is a program enabling anyone to create viruses; these will always have a lot in common. After n generations (where n is set at creation) it displays the message – 512 bytes set at creation.

Voronezh (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on opening. COMMAND.COM and COM files over 61,000 bytes are avoided.
File Growth	1,600 bytes.
Removal	Method 2.
Description	The virus contains the text `Voronezh,1990 2.01` and has no payload.

Voronezh-600 (None)

Type	Memory-resident file virus.
Affects	COM files on execution. Only files between 600 and 60,000 bytes are affected. Read-only files are not infected.
File Growth	600 bytes.
Removal	Method 2.
Description	There is no payload.

VP (None)

Type	File virus.
Affects	A COM file (selected from any subdirectory on any drive except B:) on execution of an infected file. Only files between 16 bytes and 63Kb are infected. Date/time is preserved. Critical error handling is not disabled, so attempts to infect files on write-protected diskettes are reported as errors.
File Growth	Various, calculated by rounding the size up to a multiple of 16 bytes and adding 909.
Removal	Method 1.
Description	After infection it looks at the system time. If it is in the first 5 seconds of a minute the screen is cleared and a message written to the centre (this was zeroed out in the specimen received). It waits for a keystroke, clears the screen and exits.

Vriest (None)

Type	Memory-resident file virus.
Affects	COM files on creation, for instance copying.
File Growth	1,280 bytes.
Removal	Method 1.
Description	On any day after May 3rd 1991, when a program terminates or goes TSR the virus displays `Something's coming up...` and makes a descending sound. It then displays `Vriest of g greets Vic ear Moeli~`.

Warrior (None)

Type	File virus.
Affects	An EXE file on execution of an infected file.
File Growth	1,024 bytes.
Removal	Method 1.
Description	The text `*.txt` can be found in the virus; this is patched to `*.exe` at run time to search for files to infect. While an infected program is running, any file write will write the message into the file instead. The message is: `... and justice for all! (US Constitution) Dream Over ... And the alone warrior is warrior. The powerfull WARRIOR!`

Whale (Motherfish)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	9,216 bytes.
Removal	Method 2.
Description	This virus is so large and clumsy that on most computers it doesn't actually work at all. As a result, the main replication method is anti-virus researchers sending specimens to each other. With careful treatment it can be persuaded to go TSR and infect files from memory. The system slows down considerably because the virus is so inefficient. It contains a few dozen 'heads' which are the different decryption/loader routines.

Wisconsin (None)

Type	File virus.
Affects	A COM file on execution of an infected file. COMMAND.COM is avoided.
File Growth	825 bytes.
Removal	Method 1.
Description	If the year is not 1989, every fifth time an infected program is run it displays the message `Death to Pascal` and deletes every PAS file, displaying a dot as each file is deleted.

Witcode (None)

Type	Memory-resident file virus.
Affects	EXE files on execution. Critical error handling is not disabled, so an attempt to infect a file on a write-protected diskette will be reported as an error.
File Growth	966 to 981 bytes.
Removal	Method 1.
Description	Various effects are triggered on exit from any program, whether infected or not, while the virus is in memory. Between 10pm and 6am there is a 1 in 16 chance that it will display `Gee, I wanna sleep now!`. Between December 24th and 31st it displays `Merry Christmas!`. On Sundays there is a 1 in 32 chance that it will display `You really shouldn't work on Sundays...`. On any Friday 13th and any Monday, there is a 1 in 64 chance of the payload triggering. This patches the first two bytes of the boot sector of drive C: so than hard disk becomes non-bootable.

Wolfman (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	2,064 bytes.
Removal	Method 1.
Description	The virus contains the text `Wolf_mAN`. On the 15th the payload triggers. This is supposed to overwrite the hard disk, but it just hangs the system.

WW-217 (None)

Type	File virus.
Affects	A COM file on execution of an infected file.
File Growth	217 bytes.
Removal	Method 1.
Description	The last two bytes of an infected file are `WW`.
Variants	***WW217a*** is a minor variant.

WWT-01 (None)

Type	Overwriting file virus.
Affects	All COM files in the same directory on execution of an infected file. Date/time and read/write attributes are not preserved.
File Growth	None. The first 67 bytes are overwritten.
Removal	Method 2.
Description	Programs no longer function.
Variants	**WWT-02:** 125 bytes are overwritten. Date/time and read/write attributes are preserved.

XA1 (Tannenbaum; Weinacht)

Type	File virus.
Affects	A COM file in the current directory on execution of an infected file. Only files between 7 and 63,487 bytes are affected. Date/time and read/write attributes are preserved. IBMBIO.COM and IBMDOS.COM are avoided.
File Growth	1,539 bytes.
Removal	Method 1, and then if the payload has triggered, Method 3.
Description	On April 1st the partition sector of the hard disk is replaced with the virus code, which also replaces the boot sector on drives A: and B:. Thereafter, when the computer is started the message `April, April ...` is displayed, then the computer beeps and hangs. Between December 24th and 31st it displays a Christmas tree and the message `Und er lebt doch noch : Der Tannenbaum! Frohe Weihnachten ....` This was found in Germany, hence the language. The April message is the equivalent of April Fool, and the other message (Christmas Tree! And it lives still) may be a reference to the Christmas exec worm which went through the IBM network at the end of December 1987.

Xmas (None)

Type	File virus.
Affects	A COM or EXE file on execution of an infected program.
File Growth	2,764 to 2,779 bytes.
Removal	Method 2.
Description	The virus is encrypted. If an infected file is run on December 25th, occasionally a Christmas message will be displayed. This consists of four lighted candles and `M E R R Y  C H R I S T M A S !` at the bottom of the screen. At the same time it plays the Tannenbaum carol. In the run-up to Christmas, the number of lighted candles grows from one to four. This is another version of ***Syslock***.

XPEH.4016 (XPEH, XPEH4, XPEH5, Micropox)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution or search for via DOS Find First/Find Next calls. COM files shorter than 288 bytes and longer than 61,815 bytes are not infected, neither are COMMAND.COM or AIDSTEST.EXE (a popular Russian anti-virus program).
File Growth	4,016 bytes.
Removal	Method 2.
Description	This virus uses several layers of complex self-encryption and demonstrates certain anti-bugging techniques. The name XPEH is, in fact, in Cyrillic and is pronounced 'hren'. This is Russian for 'horse radish', but is often used in Russian swearing to mean something rather different. The virus was designed not to activate until March 1991, being presumbaly distributed passively before this date, for instance by software copying and downloading from a BBS. Due to a bug, the virus is inactive in January and February of any year. At other times, on execution of an infected program the virus stays memory-resident and infects COM and EXE files being executed or looked for with the DOS Find First/Find Next calls, with a probability of 1/4 (i.e. approximately one in every four files). The virus is semi-stealth – the growth of infected files is concealed. Starting in September 1991, if a file with no extension or an extension of BAK, LEX or TXT is found via the DOS call Find First/Find Next, the virus can trash the file's contents on approximately one in four occasions. Every four consecutive bytes of a trashed file are XORed with the hex patttern 90958D85, which stands for XPEH in the Russain alternative Cyrillic character coding.
Variants	There are eight known variants. They differ in activation and trigger dates, file growth, and encryption complexity. Some do not trash text files and are able to infect COMMAND.COM. One of the latest variants contains the following encrypted Russian message: `Further development of XPEHs is suspended due to the virus author getting a permament job.`

Yale (Alameda; Merritt; Peking; Seoul; Yale Boot)

Type	Memory-resident boot sector virus.
Affects	Diskette in drive A:. When the computer is booted from an infected (non necessarily bootable) floppy, the virus goes TSR. When the diskette is replaced and Ctrl Alt Del pressed, the keystrokes are intercepted and the replacement diskette is infected. The virus takes 1Kb of RAM.
File Growth	N/A
Removal	Method 3.
Description	The original boot sector is moved to track 39, side 0, sector 8; any data is overwritten. The virus contains code for formatting track 39, but an essential part is missing in all known versions so the format doesn't happen.

Yankee-1202 (AF00-1202)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution. Files must be larger than 6,144 bytes, and COM files smaller than 63,822 bytes.
File Growth	1,202 bytes.
Removal	Method 1.
Description	There is no payload.

Yankee Doodle (Vacsina)

Type	Memory-resident file virus.
Affects	COM files on loading; EXE files smaller than 63Kb are first converted to COM files (without a name change) and then infected the next time they are executed. Read/write attributes are preserved, but date/time isn't.
File Growth	COM: 1,207 to 1,213 bytes. Converting EXE to COM files grows them by typically 132 bytes.
Removal	Method 1.
Description	When a file is infected drive A: is accessed, even if the infected program doesn't. There is no payload, other than a beep when a COM file is infected.
Variants	There are 16 versions, each with a different file growth, including several ***Vacsina*** variants; there is little functional difference from the original. In the case of the ***Vacsina*** variants, both COM and EXE files are infected and grow from 2,772 to 2,900 bytes. Date/time is preserved. At 5pm the virus plays Yankee Doodle.

Yaunch (None)

Type	File virus.
Affects	An EXE file on execution of an infected file.
File Growth	2,650 to 3,020 bytes.
Removal	Method 2.
Description	On June 17th two hearts appear at the top of the screen, then move apart, down, and together again to the centre. The message `Yaunch + Wench` is displayed surrounded by hearts.

Yukon (None)

Type	Overwriting file virus.
Affects	All COM files in the same directory on execution of an infected file.
File Growth	None. The first 151 bytes are overwritten.
Removal	Method 2.
Description	Infected programs no longer work. The virus contains the text `Divide Overflow` which is displayed when an infected file is run. The program then exits.

Zero-hunt1 (Minnow)

Type	Memory-resident file virus.
Affects	COM files on execution.
File Growth	None.
Removal	Method 1.
Description	The virus attempts to hide its infection of a file, filtering out the additional code when a program tries to read an infected file (stealth). If the virus mistakes an uninfected file for an infected one, reading that file will give the wrong results.

Zero-hunt2 (None)

Type	Memory-resident file virus.
Affects	A COM file when a directory change is made.
File Growth	None. Overwrites 416 bytes.
Removal	Method 1.
Description	The virus looks for a group of 416 zeroes, then overwrites these with itself. If the virus is in memory it conceals the change by substituting zeroes when the file is read.

Zero-to-O (None)

Type	Overwriting file virus.
Affects	A COM file on execution of an infected file.
File Growth	None. Overwrites 403 bytes.
Removal	Method 2.
Description	Programs no longer run. Every time a program is run, every 0 (zero) on the screen is converted to the letter O unless the screen is mono, in which case the system hangs.

Zero Bug (Zero Eater; Zbug)

Type	Memory-resident file virus.
Affects	Any copies of a COM file during creation. Read/write attribute is preserved.
File Growth	1,536 bytes. This is concealed if the virus is in memory.
Removal	Method 1.
Description	The virus triggers a screen display with a face (ASCII character 1) eating all the zeroes, starting at the top left and working its way down from left to right. Zeroes are replaced by spaces.

Zerotime (V1721; Slow; Sydney)

Type	Memory-resident file virus.
Affects	EXE and uninfected COM files on execution. Date/time and read/write/hidden attributes are preserved on COM files. COMMAND.COM is avoided.
File Growth	COM: 1,721 bytes. EXE: rounded to a multiple of 16 bytes then 1,716 added.
Removal	Method 1.
Description	Some EXE files are not infected correctly and fail to run. Every Friday in 1991 and after, whenever any file is closed the file timestamp is set to zero. It looks as though the author intended the date to be set to zero as well, but it is set to whatever is in the DX register. This usually means the date is zeroed, but not always. This is a variant of ***Jerusalem***, with variable encryption. Misinfections of EXE files are possible because of the faulty way in which the virus distinguishes between COM and EXE files.

Zherkov (None)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution or opening. Only files smaller than 64,512 bytes are affected.
File Growth	1,018 to 2,970 bytes.
Removal	Method 2.
Description	The strings `Welcome to demo version (C) Zherkov` and `AIDSTEST` can be found in the virus, and the whole virus is encrypted. If any floppy disk is formatted in drives A: or B:, the BIOS parameter block will be patched to reflect zero heads. If you access a floppy disk this will be concealed so that the BIOS read gives two heads. The same diskette may not work on an uninfected computer because of the error in the BIOS parameter block. If a program called AIDSTEST.EXE is run, the message `version (C) Zherkov` is displayed and the file deleted.
Variants	***1010, 1023, 1882, 1915, 1958, 2968*** and ***2960***.

ZK900 (France; Death March)

Type	Memory-resident file virus.
Affects	COM and EXE files on execution.
File Growth	900 bytes.
Removal	Method 1.
Description	73 seconds after infecting, the virus plays the Death March, repeating it every three minutes.

Index

a204, *137*

1-in-8, *245*
10 AM, *169*
10 Past 3, *49*
1210, *196*
1260, *76*
1381, *129*
1392, *52*
15 years, *105*
1530, *86*
1554, *225*
1559, *225*
1575, *120*
1621, *73*
1661, *73*
1701, *72*
1704, *72*
1704-B, *73*
1704-C, *73*
1704-Format, *73*
17Y4, *73*
1801, *86*
1813, *133*
1af, *137*

2153, *113*
2343.a, *113*
2343.b, *113*
2e7, *137*

3066, *231*
348, *248*
3503, *137*
353, *248*
3551, *223*
367, *248*

4096, *115*
423, *254*
435, *247*
4K, *115*

510, *247*
512
family, *86*
528, *247*
52f, *137*
535, *247*
555, *196*
582, *247*
583, *247*
5a4, *137*

622, *247*
623, *247*
627, *246*
637, *243*
644, *246*
645, *246*
646, *246*
646b, *246*
648, *245*, *246*
648-Lisbon, *153*
656, *246*
65d6, *137*
666, *176*
6d46, *137*

716, *246*
733, *246*
7c01, *137*

805, *213*
822, *245*

9.8min, *145*
941, *95*
9800:0000, *225*

Advert, *191*
AF00-1202, *263*
Agiplan, *166*
Aids, *49*
Aircop, *50*
AircopNG, *50*
Aircot, *50*
Akuku, *50*
Akuku-b, *50*
Akuku-c, *50*
Alabama, *51*
Alameda, *263*
Ambulance, *52*
Amoeba, *52*
Anarkia, *135*
Anarkia.2, *137*
Angelina, *53*
Anti-Pascal, *56*
Anticad, *57*
Antichrist, *162*
AntiCMOS, *54*
AntiEXE, *55*, *83*
AP-nnn, *56*
see Anti-Pascal
Arab, *58*
ARARA, *59*
Armagedon, *59*
Ashar, *69*
AT144, *60*
Attention, *60*
Australian, *214*
Austrian, *245*
Autumn, *72*
Azusa, *60*

B.4, *103*
b0f, *137*
B1, *103*, *177*
Backfont, *61*
Backfont-905, *61*
Backtime, *61*
Bad Boy, *62*
Bad Boy.a, *62*
Bad Boy.b, *62*
Bad Guy, *62*
Bandit, *63*
Bebe, *63*
Beeper, *201*
Best Wishes, *64*
Best Wishes 1, *64*
Better World, *65*
family, *66*

Bhaktivedanta, *220*
Big Italian, *187*
Big Joke, *66*
Black Avenger, *85*
Black Friday, *133*
Black Hole, *133*
Black Monday, *66*
family, *65*
Blackjack, *72*
Blackjec, *67*
Blackjec 3, *67*
Blackjec 4, *67*
Blackjec 5, *67*
Blackjec 6, *67*
Blackjec 7, *67*
Blackjec 8, *67*
Blackjec 9, *67*
Blink, *113*
Bljec, *67*
Blood, *68*
Bloody, *142*
Boot droppers, *68*
Botany, *103*
Bouncing Ball, *187*
Bouncing dot, *187*
Boys-500, *68*
Brain, *69*
cleaner, *71*, *173*
family, *194*
overwriter, *93*
Brainy, *70*
BSA, *137*
Burger, *70*
Burger-405, *70*
Burger-Pascal, *177*

Canadian, *103*
Cansu, *241*
Cara, *71*
Carfield, *137*
Carioca, *71*
Cascade, *72*
family, *138*
Casino, *74*
Casper, *75*
family, *76*
Catman, *76*
Cemetery, *162*
Century, *115*
Chameleon, *76*
family, *75*, *241*
Chaos, *77*
Charlie, *245*
Chinese Fish, *78*
Choinka, *79*
Cinderella, *79*
Clipper, *80*
CMOS4, *55*
Columbus Day, *89*
Com2Con, *80*
Computer Ogre, *178*
Cookie, *223*
Cookie-2232, *223*
Copmpletely, *50*
Cracker Jack
virus source, *62*, *92*, *104*, *108*, *131*, *156*, *163*
Crazy Daisy, *81*
Crazy Eddie, *82*
Crew 1, *82*
Crew 2, *82*
Critical, *137*

D1, *103*
D2, *103*
D3, *55*, *83*
Damage, *83*
Damage-b, *83*
Damien, *215*
Danish Tiny, *84*
Dark Avenger
family, *220*
Dark Avenger 1800, *85*
Dark Avenger 2, *86*
Dark Avenger 2000, *86*
Dark Avenger 2100, *86*
Dark Avenger Slowdown, *87*
Dark Lord, *87*
Darth, *88*
Darth Vader-2, *88*
Darth Vader-3, *88*
Darth Vader-4, *88*
Datacrime 1, *89*
Datacrime 1b, *89*
Datacrime 2, *89*
Datacrime 2b, *89*
Datalock, *90*
David, *90*
Dazzler, *138*
Dbase, *91*
DBF, *91*
Death March, *268*
December 24th, *127*
Deicide, *92*
Deicide-2, *92*
Demon, *92*
Den Zuk
family, *159*
Den Zuk 1, *94*
Den Zuk 2, *93*
Den Zuk 3, *94*
Denzuk
dropper, *68*
Destructor, *94*
Devil's Dance, *95*
Devil's Dance.b, *95*
Dewdz, *95*
Diamond, *96*
Diamond-b, *96*
Diamond-Damage, *83*
Diamond-David, *90*
Diamond-Greemlin, *119*
Diamond-Lucifer, *156*
Diana, *85*
Die Young, *86*
Dir, *97*
DIR II, *96*
Dirvir, *97*
Discom, *97*
Disk crunching, *127*
Disk eater, *127*
Disk Filler, *98*
Disk Killer, *178*
Disk Ogre, *178*
Do nothing, *217*
Donald, *215*
DoomII.1240, *99*

DoomII.752, *99*
DOS-62, *245*
DOS-68, *245*
Doteater, *100*
Dragon, *137*
DSME.Teacher, *100*
DSME:Demo, *100*
Durban, *204*
Dutch-555, *196*
Dyslexia, *101*
dropper, *101*
Dyslexia dropper, *101*

Eddie-1, *85*
Eddie-4, *86*
Eddie 2, *86*
Eddie 3, *86*
EDV, *102*
Eight Tunes, *103*
Empire, *103*
Empire.Monkey.A, *104*
Empire.Monkey.B, *104*
Enigma, *104*
Enigma.b, *104*
Espejo, *105*
Etc, *106*
Evil, *86*, *103*, *106*
Evil Empire, *103*
Exe_Bug, *107*
Exebug
dropper, *107*
Exebug.a, *107*
Exterminator, *108*

F-You, *108*
F1-337, *109*
Faggot, *109*
Falling Letters Boot, *110*
Faust, *77*
FaxFree, *167*
Feb-7th, *137*
Fellowship, *65*
see Better World
ffd, *137*
Fichv, *110*
Filedate 11, *111*
Filehider, *111*
Filler-6, *98*
First Austrian, *245*
Fish, *112*
Fish Boot, *78*
Fish6, *112*
family, *144*
Flag_ee, *137*
Flash, *113*
Flip, *113*
Flushed, *215*
Form, *114*
France, *268*
Free love, *181*
French Boot, *140*
Frère, *133*, *135*
Friday-13th-440, *179*
Friday-15th, *136*
Friday 13th, *133*, *254*
Friday15, *137*
Frodo, *115*
family, *144*
Frodo-b, *115*
Frogs, *116*
Fu Manchu, *116*
Fumble, *117*
Fumble.b, *117*

Gergana, *117*
Ghost, *118*
Ghostballs, *118*
GP1, *119*
Greek, The, *59*
Greemlin, *119*
Green Caterpillar, *120*
Grither, *245*
Grither, The, *245*
Grower-268, *120*
Guppy, *120*

Hacker, *123*
Hacker 2, *123*
Hacker 3, *123*
Hacker 4, *123*
Hacker 5, *124*
Hacker 6, *124*
Hacker 7, *124*
Hailstorm, *72*
Hallöchen, *121*
Hammer, *57*
Happy New Year 1600, *172*
Harare, *218*
Hate, *121*
Hawaii, *214*
Headcrash, *122*
Hebrew University, *133*
Hello 1a, *121*
Hemp, *214*
Hero, *122*
Hidden, *115*
HIV-1, *131*
Holland, *222*
Holland Girl, *222*
Hong Kong, *222*
Horse, *123*
dropper, *68*
Horse 2, *123*
Horse 3, *123*
Horse 4, *123*
Horse 5, *124*
Horse 6, *124*
Horse 7, *124*
Horse Boot, *124*
Hungarian-482, *124*
Hybryd, *125*
Hymn, *126*
Hymn-2144, *126*

Icelandic, *127*
Icelandic 1-b, *127*
Icelandic 2, *127*
IDF, *115*
In love, *215*
Incom, *128*
Int13, *128*
Internal, *129*
Invader, *57*
Irish, *158*
Iskey, *198*

Israeli, *133*
Italian, *187*
cleaner, *71*
dropper, *118*
family, *194*
Itavir, *130*
IVL, *131*

J, *137*
Jabberwocky, *131*
Jack Ripper, *200*
Jan25, *137*
Japanese Christmas, *132*
Jeff, *132*
Jerspain, *135*
Jeru-Carfield, *137*
Jeru-Clipper, *80*
Jeru-Discom, *97*
Jeru-GP1, *119*
Jeru-Kylie, *148*
Jeru-Spanish, *135*
Jeru-Sunday, *134*
Jerusalem, *133*
family, *57*, *65*, *66*, *77*, *80*, *97*, *116*, *119*, *121*, *148*, *168*, *172*, *184*, *204*
Jerusalem-113b, *135*
Jerusalem-Apocalypse, *135*
Jerusalem-B, *133*
Jerusalem-Captain Trip, *136*
Jerusalem-Czech, *135*
Jerusalem-Frère.2, *136*
Jerusalem-J, *136*
Jerusalem-Jan25, *136*
Jerusalem-Nemesis, *136*
Jerusalem-Sat13, *136*
Jerusalem-T1, *135*
Jerusalem-T13, *136*
Jerusalem-Westwood, *135*
Jerusalem-Yellow, *136*
Jerusalem Mendoza, *137*
Jocker, *138*
Jojo, *138*
Joker, *138*
Joker-01, *139*
Joshi, *139*
Joshua, *139*
July 13, *140*
Jumper, *140*
June 16th, *141*
June 4, *142*
June 7, *132*
Junkie, *143*
Justice, *143*
JV, *133*
JVT1, *137*

Kamasya, *144*
Kampana-3445, *144*
Kampana-boot, *225*
Kemerovo, *145*
Kennedy, *84*
Keydrop, *145*
Keypress, *145*
Keytrick, *146*
Khetapunk, *52*
Kiev-483, *146*
Kitty, *146*
Klaeren, *121*
Korea, *173*
Kranz, *222*
Kukac-Nagytud, *147*
Kukac Turbo, *147*
Kylie, *148*

Lahore, *69*
Laodung, *215*
Lazy, *148*
LBC, *173*
Leapfrog, *149*
Leech, *149*
Lehigh, *150*
Lenart, *54*
Leprosy, *151*
family, *192*
Leprosy-B, *151*
Leprosy-C, *151*
Leprosy-D, *151*
Leprosy.Busted, *151*
Leszoptad, *152*
Liberty, *152*
Liberty.b, *152*
Liberty.c, *152*
Lisbon, *153*
Lisbon.b, *153*
Lisbon.c, *153*
Lisbon.d, *153*
Little Pieces, *154*
Live after Death
family, *174*
Live after Death 1, *154*
Live after Death 2, *155*
Live after Death 3, *106*
Live after Death 4, *186*
Live after Death 5, *195*
Lovechild, *156*
Lucifer, *156*
Luz, *191*

Macho, *223*
Macrosoft, *223*
Magnitogorsk, *157*
Magnitogorsk-2048, *157*
Maltese Amoeba, *158*
Many Fingers, *159*
Mardi, *159*
Marijuana, *214*
Mendoza, *137*
Merritt, *263*
Messina, *137*
Mexican, *95*, *215*
MG, *159*
MG1, *159*
MG2, *159*
MG3, *159*
MGTU, *160*
Michelangelo, *160*
Microbe, *161*
Micropox, *262*
Migram, *162*
Migram-Cemetery, *162*
Migram-Smack, *163*
Milena, *86*
Milous, *175*
Minnow, *265*
Minsk-1075, *163*
MIR, *86*
Mirror, *164*

Mistake, *187*
Mix 2, *166*
Mix1, *165*
Mix1-b, *166*
Mixer1, *165*
MLTI, *198*
Monkey, *104*
Month 4-6, *166*
Monxla, *167*
Morbus Waiblingen, *133*
Mosquito, *167*
Motherfish, *257*
Mule, *168*
Murphy, *169*, *218*
Murphy-1, *169*, *170*
Murphy-2, *169*, *170*
Murphy-3, *170*
Murphy-4, *170*
Music virus, *182*
Musicbug, *170*
Musician, *182*

Nagytud, *147*
Natas, *171*
Naughty Hacker, *123*
Necrophylia-b, *172*
Necropolis, *172*
New York Boot, *177*
New Zealand, *214*
NewBug, *55*
Nina, *172*
Nina-256, *173*
Nina 2, *173*
NJH, *173*
NJH-LBC, *173*
No Bock, *174*
Nocargar, *191*
Noint, *215*
Nomenklatura, *174*
Nomenklatura.b, *174*
Non-Canadian, *103*
Noon-beep, *175*
Not13, *137*
NotB, *176*
Nov30, *137*
Nulls, *215*
Number 1, *49*
Number 1.b, *177*
Number of the Beast, *176*
Number One, *177*
NYB, *177*

Ogre, *178*
dropper, *68*
Ohio, *94*
Old Yankee, *179*
plagiarism, *104*
Omega, *179*
Omicron, *113*
ON 64, *180*
One Half.3544, *181*
Ontario, *182*
Oropax, *182*

Pakistani, *69*
Pakistani Brain, *69*
Paris, *182*
Parity, *183*
Parity boot, *183*
Pathogen, *209*, *210*
Payday, *133*
PcDrsVs, *184*
Peking, *263*
Perfume, *185*
Perfume-731, *185*
Perfume.blank, *185*
Perfume.message, *185*
Perfume.Slash, *185*
Phenomen, *137*
Phoenix 1226, *155*
Phoenix 800, *154*
Phoenix Evil, *106*
Phoenix phoenix, *186*
Phoenix Proud, *195*
Ping Pong, *187*
cleaner, *173*
similarities, *131*
Ping Pong-B, *187*
Piter, *188*
Pixel, *189*
Pixel-275, *191*
Pixel-277, *191*
Pixel-283, *191*
Pixel-295, *191*
Pixel-299, *190*
Pixel-345, *190*
Pixel-779, *190*
Pixel-837, *190*
Pixel-847, *190*
Pixel-850, *190*
Pixel-854, *190*
Pixel-877, *190*
Pixel-892, *190*
Pixel-897, *189*
Pixel-899, *189*
Pixel-899b, *189*
Pixel-905, *189*
Pixel-Year-6545, *191*
Plague, *192*
Plastique, *57*
Polimer, *192*
Polish, *243*
Possessed, *193*
Possessed.b, *193*
Prague Blinker, *61*
see Backtime
Prague Joker, *61*
see Backtime
Prague Shaker, *61*
see Backtime
Pretoria, *141*
Print Screen
dropper, *68*
Print Screen-1024, *193*
Print Screen Boot, *194*
Profesor, *201*
Proud, *195*
Prudents, *196*
Ps!ko, *86*
PSQR, *135*
Puerto, *137*

Queeg, *210*
Queit, *201*
Quit-1992, *196*
Quit-1992.B, *196*
Quox, *197*

Rabid, *86*
Raubkopie, *197*
Ray Joke, *198*
RC-1049, *198*
Red Cross, *52*
Red Diavolyata, *198*
Redx, *52*
Revenge, *199*
RightShift, *232*
Ripper, *200*
Rostov, *215*
Russ-1075, *163*
Russian, *72*, *133*
Russian Mirror, *201*
RVPS, *235*

Sadam, *201*
Sampo, *202*
Samsoft, *145*
San Diego, *214*
Sanded, *214*
Saratoga, *127*
Satan Bug, *203*
Saturday 14th, *204*
Scotts Valley, *204*
Screen+1, *205*
Search, *93*
Second Austrian, *72*
Sector Zero, *205*
Sentinel, *206*
Seoul, *263*
Sex Revolution, *214*
Shadowbyte, *206*
Shake, *207*
SI-492, *207*
SillyBop, *140*
Simulate, *208*
Siskin-Hero-506, *122*
Skism, *136*
SKISM, *137*
Slow, *267*
Slowdown, *86*, *87*
Smack, *163*
SMEG.Pathogen, *209*
SMEG.Queeg, *210*
SMEG v0.1, *209*
SMEG v0.2, *210*
Smithsonian, *214*
Solano, *101*
Sonus, *215*
Spanish, *137*, *231*
Spanz, *211*
Sparse, *211*
Squeaker, *211*
St Leos, *145*
Stack, *212*
Staf, *212*
Standard.AA33CCDDEE, *137*
Standard.Nocommand, *137*
Standard.null, *137*
Standard.SuMsdos, *137*
Standard.UMsDos, *137*
Standard.Var, *137*
Stardot-600, *213*
Stardot-789, *213*
Stealth, *197*
Stoned, *214*
cleaner, *71*
detected by V-Sign, *241*
dropper, *216*
family, *142*, *160*, *194*
Stoned-16, *215*
Stoned-8, *215*
stoned-floppy, *215*
Stoned.Angelina, *53*
Stoned dropper, *216*
Striker, *216*
STSV, *216*
Stupid, *217*
family, *201*
sUMFDos, *137*
sUMsDOS, *133*
Sunday, *134*
Sunday.b, *134*
Sunday 1.b, *134*
Sunday 1.d, *134*
Sunday 1 Tenseconds, *134*
Sunday 2, *134*
Suomi, *217*
Superhacker, *218*
Suriv, *134*
SVC, *219*
SVC 3.1, *219*
SVC 5.0, *219*
SVC 6.0, *219*
Sverdlov, *126*
SVIR, *220*
Swami, *220*
family, *131*, *144*, *162*
Swedish Disaster, *214*
Swiss-143, *221*
Sydney, *267*
Sylvia, *222*
Syslock, *223*
family, *261*

Taiwan, *57*
Taiwan-708, *224*
Taiwan-743, *224*
Taiwan DoomII.1240, *99*
Taiwan DoomII.752, *99*
Talentless Jerk, *218*
Tannenbaum, *260*
TCC, *182*
Telefonica
dropper, *144*
Telefonica-boot, *225*
Tenbytes, *225*
Tenbytes-1554, *225*
Tequila, *226*
Teraz, *215*
Terror, *226*
Testvirus B V1.4, *227*
Thanksgiving, *228*
The Greek
see Anti-Pascal

The Rat, *228*
Thirteen minutes, *229*
Thursday-12th, *229*
Tiny, *229*, *230*
family

Tiny-123, *230*
Tiny-127, *230*
Tiny-128, *230*
Tiny-Mutant, *230*
Topsy-905, *61*
Traceback, *231*
Traceback-2930, *231*
Trackswap, *231*
Trash, *232*
Traveller, *86*
Tremor, *233*
Trivial, *234*
Tumen, *234*
Tumen.1092, *235*
Tumen.1242, *235*
Tumen.1255, *235*
TUQ, *235*
Turbo, *202*
Turin, *187*
Turkish, *137*
Twelve Tricks, *236*
Twin, *239*
Twins, *145*
Two Tigers, *136*
Type, *117*
Typo, *187*
Typo Com, *117*
Typoboot, *187*

U of A, *103*
UA, *103*
UIUC, *69*
Unesco, *245*
Uruguay.1, *240*
Uruguay.2, *240*
Uruguay.3, *240*
Uruguay.4, *240*
Uruguay.5, *240*
Uruguay.6, *240*
Uruguay.7, *240*
Uruguay.8, *240*
Uruguvau, *240*
Usenet, *225*
USSR, *111*
USSR-1049, *198*
USSR-707, *240*

V-277, *191*
V-Sign, *241*
V1024, *96*
V1028, *87*
V1226, *155*
V1253, *228*
V1600, *172*
V1721, *267*
V200, *216*
V2000, *86*
V2100, *86*
V2480, *82*
V257, *145*
V270X, *120*
V2P2
family, *76*
V2P6, *241*
family, *76*
V512, *176*
V516, *149*
V696, *180*
V707, *240*
V711, *229*
V789, *111*
V905, *61*
V948, *205*
Vacsina, *264*
Valert, *225*
Vbasic, *242*
Vbasic.B, *242*
Vbasic.C, *242*
Vcomm, *243*
Vcomm.A, *243*
VCS, *254*
VDV-853, *243*
Venezuelan, *93*
Vera Cruz, *187*
VFSI, *244*
Victor, *244*
Vienna, *245*
family, *79*, *125*, *153*, *167*, *211*, *248 - 251*
Vienna-1881, *79*
Vienna-534, *248*
Vienna-648, *245*
Vienna-71a1, *245*
Vienna-774, *245*
Vienna-Iraqui, *249*
Vienna.W13B, *248*
Violator, *250*
Violator-Arf, *251*
Violator-arf.2, *251*
Violator B3, *250*
Violator B4, *251*
Virdem, *252*
Virdem-1542, *252*
Virdem.2, *252*
Virdem Disktrash, *252*
Virdem English, *252*
Virus-101, *253*
Virus-90, *253*
Virus-B, *254*
Virus Construction Set, *254*
Voronezh, *255*
Voronezh-600, *255*
VP, *255*
Vriest, *256*

W13.A, *248*
W1lop, *202*
Wabik, *138*
Warrier, *70*
Warrior, *256*
Waterfall, *72*
WDn, *215*
Weinacht, *260*
Westwood, *135*
Whale, *257*
Wisconsin, *257*
Witcode, *258*
Wolfman, *258*
Wonderful, *252*
WW-217, *259*
WW217a, *259*
WWT-01, *259*
WWT-02, *259*

XA1, *260*
XBoot, *231*
Xmas, *223*, *261*
XPEH, *262*
XPEH.4016, *262*

XPEH4, *262*
XPEH5, *262*
Xswap, *231*

Yale, *263*
Yale Boot, *263*
Yankee-1202, *263*
Yankee Doodle, *264*
Yaunch, *264*
Yukon, *265*

Zapper, *214*
Zbug, *266*
Zero-hunt1, *265*
Zero-hunt2, *265*
Zero-to-O, *266*
Zero Bug, *266*
Zero Eater, *266*
Zerotime, *267*
Zherkov, *268*
ZK900, *268*

Dr. Alan Solomon

Dmitry O. Gryaznov

Viruses: The Facts

Based on virus disassemblies and analysis carried out by Dr. Alan Solomon, the world's foremost computer virus researcher, this is the most concentrated source of facts about PC viruses ever published. Usable, pertinent facts, not theory or speculation.

The viruses you are likely to meet in the real world are covered in this book. This is the information you need to deal with them on your own terms.

Alan Solomon is a founder member of the Computer Anti-Virus Research Organisation (CARO) and was the first technical director of the European Institute for Computer Anti-Virus Research (EICAR). He is director of Research & Development and Chairman of S&S International, developers of the world-renowned Dr Solomon's Anti-Virus Toolkit.

Dmitry O. Gryaznov was a Research Scientist at the Program Systems Institute, Russian Academy of Sciences. Gryaznov, a member of CARO, did ground-breaking research into viruses in the USSR, and is a regular speaker at anti-virus conferences world-wide. He works at the S&S International Virus Lab as a Senior Virus Research Analyst.

S & S
INTERNATIONAL PLC

Alton House, Gatehouse Way, Aylesbury, Bucks HP19 3XU. United Kingdom
Tel: +44 (0)1296 318700 Sales Tel: +44 (0)1296 318800 Sales Fax: +44 (0)1296 318888
e-mail: support@sands.co.uk

2101A-00-00-7.0